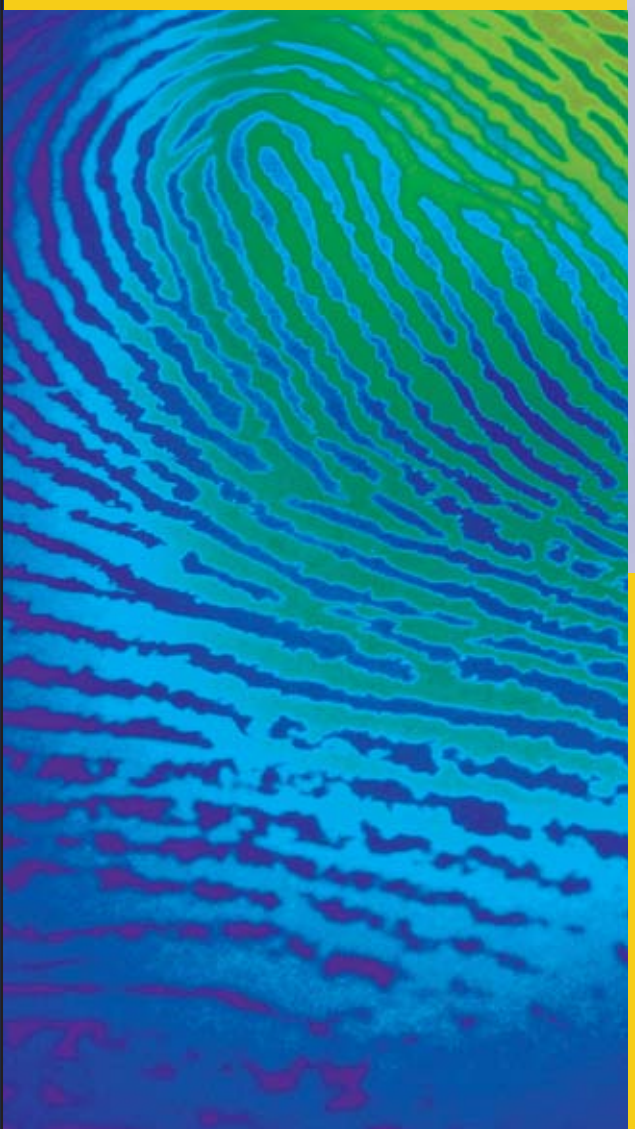
The forensic use of bioinformation: ethical issues



NUFFIELD COUNCIL ON BIOETHICS

Executive summary

Introduction (Chapter 1)

1 The development over the past two decades of the science of deoxyribonucleic acid (DNA) profiling has led to a dramatic increase in the forensic use of bioinformation. Together with the older use of fingerprints and other emergent biometric technologies, there is growing potential for combining data to produce multi-modal identification systems. Police powers to take and retain fingerprints and biological samples have been steadily widened by a series of Acts of Parliament. Today the police of England and Wales have wider sampling powers than those in any other country, and the United Kingdom has proportionally, per head of population, the largest forensic DNA database in the world, with approximately four million samples (or about six per cent of the population), while the national fingerprint database holds over 6.5 million fingerprint records from individuals.

The interpretation of bioinformation (Chapter 2)

2 Recent cases have highlighted concerns about fingerprinting techniques, and there is controversy over the standard required before a true 'match' between a fingerprint found at a crime scene and one taken from a suspect can be declared. However, once a match is made, fingerprint evidence generally remains unassailable in the criminal courts as a unique identifier (see paragraph 2.2).

3 In general, the science and technology of DNA profiling is increasingly robust and reliable. However, there remain risks, especially when the scientific techniques are pushed to their limits. In particular there are dangers of deliberate or accidental contamination, misinterpretation of mixed samples (those originating from more than one person), mistaken interpretation of partial profiles and the misuse of statistics to establish the probability of a match. Our recommendations in the following chapters are designed to reduce the risks of mistaken identification resulting from (relatively rare) cases of flawed science. We also recommend that the regulatory authorities should require and rigorously monitor quality assurance, and support independent research into new scientific techniques and technologies that are likely to improve reliability and accuracy.

Ethical values and human rights (Chapter 3)

4 The protection of the public from criminal activities is a primary obligation of the state. In a liberal democracy, such as the United Kingdom, it is also necessary to protect several fundamental ethical values and to respect modern legislation on human rights. The values with which we are primarily concerned are *liberty, autonomy, privacy, informed consent* and *equality*. These values are not absolute but there is a strong presumption in liberal democracies in favour of not restricting them. We broadly endorse a rights-based approach that both recognises the fundamental importance to human beings of respect for their individual liberty, autonomy and privacy, and the need, in appropriate circumstances, to restrict these rights either in the general interest or to protect the rights of others.

5 It is clear that well-functioning forensic databases have the potential to promote the public interest to a significant degree, but to argue convincingly that this justifies overriding identifiable personal interests or rights requires a number of further steps. The principle of *proportionality*, which is relevant in both ethical and legal debates, is thus at the heart of many of the recommendations in this Report. The legally enforceable human rights that are relevant to our justifications include the right to a *fair trial*, the right to *respect for private*

and family life, and the right to *equal treatment*. Any interference with these rights must be *proportionate*.

Criminal investigation (Chapter 4)

Taking fingerprints and biological samples

6 Fingerprints and DNA samples may be taken from suspects, victims or witnesses in the course of criminal investigations. If an individual has been arrested in connection with a 'recordable' offence[1], the present law in the United Kingdom permits the police discretion to take fingerprints and biological samples without the consent of the individual. Many of those arrested for these offences may have committed other offences. Thus the taking of samples from them raises the possibility of identifying suspects for unsolved prior offences from which biological material was obtained. **It is our view that the authority to take (for impending use in criminal investigation) fingerprints and biological samples without consent from those who are arrested on suspicion of involvement in any recordable offence is proportionate to the aim of detecting and prosecuting crime. At the same time, we note that the distinction between recordable and non-recordable offences is to some extent arbitrary (e.g. failing to give advance notice of a procession is recordable, but obstruction of the highway is not). We recommend that the list of recordable offences for which fingerprints and biological samples can be taken from arrestees, should be rationalised so as to exclude all minor, non-imprisonable offences** (paragraph 4.17).

7 Home Office proposals announced in March 2007 suggested that the police may in future be permitted to take and store fingerprints and biological samples from any arrestee, regardless of whether or not the offence was recordable. This would extend sampling to people who may have been arrested on suspicion of minor offences, such as minor traffic offences, littering or begging. With this potential further extension of police powers, the National DNA Database (NDNAD) could expand dramatically, rapidly encompassing a fifth or more of the population. **It is our view that the authority of the police to take and store both fingerprints and biological samples from all arrestees without their consent, regardless of the reason for the arrest, is disproportionate to the aims of identifying a person and of confirming whether or not a person was at a crime scene. Suspicion of involvement in a minor (at present 'non-recordable') offence does not justify the taking of bioinformation from individuals without their consent** (paragraph 4.23).

8 Police powers to take bioinformation are no longer confined to use within a police station. Indeed, the recent introduction of hand-held devices that can check fingerprints against the national fingerprint database, has led to the ability of the police to check the identification of individuals already on the database 'on-the-spot'. **Where fingerprints are taken electronically in order to verify an identity, they should be compared only with stored subject records and destroyed once such a check has been completed** (paragraph 4.23).

Retaining biological samples, DNA profiles and fingerprints

9 The retention of fingerprints, DNA profiles and biological samples is generally more controversial than the taking of such bioinformation, and the retention of biological samples raises greater ethical concerns than digitised DNA profiles and fingerprints (given the differences in the level of information that could be revealed). The Criminal Justice Act 2003 extended indefinite retention both of fingerprints and biological samples to all those

1. All offences which carry the possibility of a custodial sentence are recordable (or 'notifiable'), plus 52 other, non-imprisonable offences specified in the Schedule to the National Police Records (Recordable Offences) (Amendment) Regulations 2005 (SI 2005/3106). See Box 1.2.

arrested for recordable offences in England and Wales, even if they are subsequently acquitted. The Home Office proposals (published in March 2007) mentioned above would allow such retention from *all* arrestees. The criminal justice systems of many European countries do not have such wide powers of retention as England and Wales. For example, in Scotland indefinite retention of both the profile and the subject sample is allowed only on conviction of an offence, with the exception of time-limited retention in the case of charge for sexual or violent offences. In all other cases, samples and information derived from them must be destroyed if the arrestee is not convicted of an offence or otherwise subject to judicial disposal.

10 The retention of fingerprints or DNA profiles does not (at this time) permit the police to derive directly more detailed information about an individual. In particular, a fingerprint cannot reveal information about an individual, and the DNA profiles currently produced are limited, making it difficult for the profile to reveal further, or sensitive, information (see Chapter 2 for details). It is, however, entirely possible to sequence all or part of an individual's genome from their biological sample, and therefore, the retention of biological samples requires much greater critical attention, and justification. It is our view that electronic retention of fingerprints and DNA profiles is much less contentious than the retention of biological samples and incurs very little cost. However, there is, at present, a lack of convincing evidence that retention of profiles of those not charged with or convicted of an offence has had a significant impact on detection rates and hence it is difficult to argue that such retention can be justified. **Accordingly we recommend that independent research should be commissioned by the Home Office to assess the impact of retention. In the light of the findings of that research, an informed judgment could then be made** (paragraph 4.53).

11 Our approach to the retention of fingerprints, profiles and biological samples is guided by the principle of proportionality, bearing in mind the purpose of retaining bioinformation on the one hand, and, on the other, the absence of satisfactory empirical evidence to justify the present practice of retaining indefinitely such information from all those who are arrested for a recordable offence, irrespective of whether they are subsequently charged or convicted. We note that in Scotland and most other European countries such retention is not considered necessary. We also recognise that there are personal implications for individuals whose profiles are on the NDNAD as a result of being implicated in a crime, but who were subsequently found to be innocent (see paragraphs 3.24–3.26). Moreover, in the case of retention of samples, this is not only expensive, but it is also the focus of considerable public concern about possible future uses to which the samples might be put. **We recommend that the law in England, Wales and Northern Ireland should be brought into line with that in Scotland. Fingerprints, DNA profiles and subject biological samples should be retained indefinitely only for those convicted of a recordable offence. At present, the retention of profiles and samples can be justified as proportionate only for those who have been convicted. In all other cases, samples should be destroyed and the resulting profiles deleted from the NDNAD. This should be reviewed in the light of the findings of the further research that we have recommended** (paragraph 4.54).

12 **The Scottish practice of allowing retention of samples and profiles, for three years, from those charged with serious violent or sexual offences, even if there is no conviction, should also be followed. Thereafter the samples and profiles should be destroyed unless a Chief Constable applies to a court for a two-year extension, showing reasonable grounds for the extension** (paragraph 4.55).

13 The costs of sampling increasing numbers of individuals, maintaining an expanding database, and storing millions of biological samples will continue to escalate, yet there is little supportive empirical evidence that demonstrates significant benefits in terms of crime

detection. An alternative policy may be to dedicate more resources to developing clear auditing processes to demonstrate the worth of the NDNAD and IDENT1 (the software platform that hosts the national fingerprint database), while ensuring that there are processes in place to exploit fully the bioinformation already available to the police, and to prioritise the collection of bioinformation from crime scenes, rather than individuals. At present, fewer than 20 per cent of crime scenes are forensically examined, and only a small proportion of these yield any biological material that is then tested. **In light of the discussion of the usefulness of bioinformation in the investigation of crime, we recommend that:**

- **Expenditure for expert crime scene analysis should be given higher priority than the increased collection of subject samples. If the Government is right to assert that "the whole of the active suspect criminal population is now held on the NDNAD", then further improvements in DNA detection rates rest heavily on expanding crime scene collection rates and ensuring that full use is made of the material collected.**
- **There should be improved recording of police data on the uses of DNA matches and the production of better statistics to inform key stakeholders and the wider public. More effort should also be made to ascertain 'best practice' within policing to maximise the crime control potential of bioinformation. The collation of statistics would also assist with an exploration of the cost-effectiveness of the forensic use of bioinformation and may provide evidence as to whether infringements on the liberty, privacy and autonomy of individuals are justified.**
- **To justify the interference with the liberty and autonomy of citizens, more detailed independent research on the contribution of bioinformation to criminal justice is required** (paragraph 4.35).

14 Samples obtained from crime scenes are not currently retained once a conviction has been secured in relation to an offence and a decision has been made that it will no longer be investigated. Permanent retention of crime scene samples would permit not only the possible identification of further potential suspects who may have been involved in an offence, but also allow for the possibility of rectifying possible miscarriages of justice in the future. **We therefore recommend that, because crime scene samples are unique and unrepeatable, they must be retained indefinitely** (paragraph 4.56).

Volunteers

15 Volunteers (who may be victims, witnesses or volunteers in mass intelligence screens) may consent at the time of sampling to their profiles being permanently loaded onto the NDNAD. This decision is currently irrevocable. Such an approach is contrary to standard practice in medical research, and differs from practice in Scotland and many other European countries, where consent can be withdrawn. It has been reported to us that up to 40 per cent of people who voluntarily provide elimination samples also consent (irrevocably) to having their sample stored permanently and their profile loaded onto the NDNAD where it will be used in speculative searches for the indefinite future. If true, we believe that such a level of consent may be lower if it were fully informed and properly considered.

16 **It is our view that consent given by a volunteer to retain their biological samples and resulting profile on the NDNAD must be revocable at any time and without any requirement to give a reason. This is a basic principle in all medical research and should equally apply to the voluntary component of the NDNAD, as it already does to the Scottish DNA Database. In view of the importance of this principle, we recommend that as a matter of policy, volunteers should not be asked to consent to the permanent storage of elimination biological samples and retention of DNA profiles derived from these samples beyond the conclusion of the relevant case** (paragraph 4.62).

Ethnic minorities

17 Policing priorities and practices may lead to the disproportionate arrest of certain populations. Attention has focused in particular on the over-representation of members of black minority ethnic groups and the number of young persons (under 18) without criminal records on bioinformation databases.

18 **In our view, the disproportionate over-representation of black ethnic minorities on the NDNAD is a matter of considerable concern, even if this arises from policing practice in making arrests rather than a fault with the NDNAD. Such disparities increase the risk of stigmatisation attendant on being known to have a profile on the NDNAD and can potentially lead to further alienation of whole minority ethnic communities. We therefore welcome the commissioning of an equality impact assessment by the NDNAD. This impact assessment should reveal the extent to which it is the discretionary use of powers of arrest or the use of sampling powers that contributes to over-representation of black ethnic minorities. The NDNAD and police forces may then be put under a positive obligation to take effective steps to address this over-representation. The promotion of equality of opportunity entails active steps to remove any practices that unjustifiably cause disparities between different groups** (paragraph 4.66).

Minors

19 While it is unsurprising that young people are over-represented on forensic databases in light of the peak age of offending, this has provoked criticism. In our view, the policy of permanently retaining the bioinformation of minors is particularly sensitive in the United Kingdom, where the age of criminal responsibility is low (at age ten years in England and Wales and eight in Scotland) compared with many other countries. It may be argued that retaining bioinformation from young people is contrary to Article 40 of the UN Convention on the Rights of the Child, in that the Convention requires special attention to be given to the treatment of children by legal systems, to protect them from stigma, and that if they have offended, opportunities for rehabilitation should be maximised. The destruction of relevant criminal justice records and accompanying body samples could become one element in such a rehabilitative process.

20 **When considering requests for the removal of profiles from the NDNAD and the destruction of biological samples taken from minors (including from adults who were minors when their DNA was taken), we recommend that there should be a presumption in favour of the removal of all records, fingerprints and DNA profiles, and the destruction of samples. In deciding whether or not the presumption has been rebutted, account should be taken of factors such as:**

- **the seriousness of the offence;**
- **previous arrests;**
- **the outcome of the arrest;**
- **the likelihood of this individual re-offending;**
- **the danger to the public; and**
- **any other special circumstances** (paragraph 4.72)**.**

A population-wide database

21 There is recurrent public discussion of the potential for a population-wide DNA database, which would maximise forensic profiling abilities for the police while addressing concerns about discrimination. However, the increased intrusion into privacy that this would entail

would be compensated by only a negligible increase in public safety. In addition, there are also broader concerns that such a development would significantly shift the relationship between the individual and the state in that it might identify all individuals as potential offenders rather than as citizens of good will and benign intent.

22 **Currently, the balance of argument and evidence presented to us is against the establishment of a population-wide forensic DNA database. We conclude that such a response would be:**

- **disproportionate to the need to control crime;**
- **unlikely to secure public support; and**
- **impractical for the collection of samples from different categories of persons (such as visitors to the United Kingdom).**

However, the possibility of its establishment should be subject to review as biometric technology develops, and in the light of research on the potential contribution of such a database, under appropriate safeguards, to public safety and the detection of crime, and its potential for reducing discriminatory practices (paragraph 4.79).

Trial (Chapter 5)

23 Scientific techniques assist in the administration of justice only where the bioinformation used in a prosecution is robust, and is interpreted and represented accurately. Often it may have little or no evidential value: for example, in an assault where self-defence is raised. Further, serious doubts remain about the use of statistics in criminal proceedings. Scientific evidence, and the accompanying statistical data, may not (yet) be properly understood by non-experts involved in criminal proceedings, such as jurors, or even barristers, solicitors and judges.

24 During the pre-trial stages, in order that a defendant has the opportunity to challenge a fingerprint or DNA match, or its interpretation, it is vital that all DNA and fingerprint evidence is disclosed in a timely manner to both the defence and prosecution. Previous miscarriages of justice have highlighted the problem of non-disclosure of evidence to the defence. **We recommend:**

- **Compulsory and timely disclosure of *all* fingerprint bureau or DNA laboratory results and relevant records to all parties involved, including details of any dispute over an identification, rather than presenting only the consensus view reached.**
- **In expert witness statements and reports, this duty of disclosure should be explicitly acknowledged and the experts should confirm that they have complied with this duty** (paragraph 5.9)**.**

25 It has become clear that fingerprint evidence can no longer be presented in court as if it were a simple statement of fact that there is a match between a crime scene mark and an accused person's print. Expert evidence which identifies marks linking an accused person to a scene of crime is evidence of opinion based on examination of the materials using the skill and experience of the expert. **We recommend that in presenting their opinion regarding a positive match or otherwise to the investigating officer, prosecution authority or court, fingerprint experts should make it clear that their conclusion is always one of expert judgment, and never a matter of absolute scientific certainty** (paragraph 5.15).

26 The 'prosecutor's fallacy' has compromised the use of DNA evidence for a fair trial. This fallacy suggests that the rarity of a profile is interchangeable with the probability that the defendant is innocent (for example the rarity of a one in a million match produces the false

conclusion that the chance of the defendant being innocent is one in a million).

27 Popular media representations of the power of fingerprint or DNA evidence may exacerbate difficulties in courtrooms. There are risks that, while a DNA match cannot be used without other evidence in a prosecution, it may be given undue weight in the courts. High expectations of the significance of bioinformation in forensics make essential the proper education of legal professionals throughout the criminal justice system, to prevent the misrepresentation of evidence, or at least to ensure the recognition of flawed or misrepresented evidence.

28 **In view of the difficulties with the presentation of complex statistical information in the courtroom, we recommend:**

- **that professionals (including judges) working within the criminal justice system should acquire a minimum standard of understanding of statistics, particularly with regard to DNA evidence;**
- **that trial judges ensure statistical evidence is accurately presented during trials, and that the decision in the *R v Doheny and (Gary) Adams* (1997) 1 Cr. App. R. 369 judgment regarding the correct presentation of DNA evidence is adhered to; and**
- **that in all cases where bioinformation evidence is adduced, introductory information should be made available to jury members, to ensure some basic understanding of the capabilities, and also the limitations, of such evidence** (paragraph 5.34).

Familial searching, inferring ethnicity, and research (Chapter 6)

29 The law makes clear that bioinformation stored on forensic databases may only be used for purposes related to preventing, detecting and prosecuting crime, or identifying a deceased person or a body part. This is, however, open to wide interpretation, and thus its original use for matching DNA profiles of suspects with crime scene samples has been extended by familial searching, inferring ethnicity and non-operational research.

Familial searching

30 When a crime scene profile does not match exactly any profile on the NDNAD, it is possible to look for 'partial' matches, which might mean that the crime scene stain was left by a (genetic) relative of a person whose profile partially matches the crime scene sample. This 'familial searching' technique can produce very many possible partial matches, severely limiting its usefulness. Because familial searching identifies a pool of possible genetic relatives of a suspect, it may thus produce sensitive information about biological relationships between individuals that may be unknown to the individuals concerned.

31 The aim of familial searching may be to legitimately provide useful intelligence in crime solving and there may be instances in which its use can be justified (see paragraph 6.11). However, before the technique is implemented on a wide scale, clear and explicit guidelines on its use must be introduced and made public, with adequate safeguards to protect against any possible unwarranted intrusion into family privacy. **While we do not believe that familial searching interferes with privacy rights to an extent that should prohibit its use (see paragraphs 3.3–3.7), it is our view that the potential benefits for crime detection must be balanced carefully with any potential for harm. The lack of consent obtained when sampling makes the use of the NDNAD in searching for relatives particularly sensitive. It is important therefore that this technique is not used unless it is necessary and proportionate in a particular case. Before it is more widely deployed, there needs to be detailed and independent research on its operational usefulness and on the practical consequences for those affected by it** (paragraph 6.11).

Inferring ethnicity

32 A statistical process can be applied to a DNA profile obtained from a crime scene stain, with the aim of predicting the 'ethnic appearance' of the unidentified individual to whom the DNA profile relates. The use of such a technique provides only an inference for use during a police investigation, for example reducing the size of a suspect 'pool', priority setting, or supporting or contradicting any witness statements. Although an ethnic inference is not used as prosecution evidence, significant ethical and practical concerns remain. Drawing an ethnic inference may lead police to narrow the focus of their enquiries prematurely, and there remains an anxiety that the current system of classification of people into seven 'ethnic appearances' may reinforce existing prejudice and racist generalisations about the likely perpetrators of crime. **In view of the significant ethical and practical problems, and the limited usefulness of the information provided, attempts to infer ethnicity from DNA profiles and samples fail the test of proportionality and we recommend that ethnic inferences should not be routinely sought, and should be used with great caution** (paragraph 6.17)**.**

Non-operational research

33 Many of the uses of the NDNAD and stored samples can be classified as 'operational', in that the use is directly related to particular police investigations. However, the NDNAD and stored samples can also be used for other research purposes (in relation to forensics or crime) and in this context it is important to distinguish between the use of digital profiles and the use of the physical biological samples. Expanding use of the NDNAD makes crucial the need to introduce robust forms of ethical oversight and governance, particularly in instances where researchers use archived biological samples.

34 In deciding whether to permit research using the NDNAD and stored samples, the NDNAD Strategy Board considers whether there is a police need for the specified purpose, and the legality and ethical aspects of that purpose. Given the great sensitivity surrounding the use of genetics and the potential for harm, we recommend that any such proposals should be subjected to close ethical review. **We make a general recommendation that all research proposals using the NDNAD and stored samples should be formally, independently and transparently evaluated** (paragraph 6.21).

35 There are potentially a variety of research activities that could be performed using the resources of the NDNAD, including research into genetic markers of ethnicity, or genetically associated behavioural traits which may impact upon or influence criminality. **While recognising the potential value of research into genetic behavioural traits and ethnicity, in common with all other non-operational research, proposals in these areas must be subject to robust ethical scrutiny. The scientific credibility of the proposed research must be evaluated, examining, for example, the extent to which inherent biases in the National DNA Database may compromise the ability to identify 'causal' relationships between genetics markers and criminal behaviour and hence support misleading conclusions. Such scrutiny would need to balance any potential benefits from the research against the risks of increasing social stigmatisation and racial stereotyping, or a potential detrimental impact upon efforts to rehabilitate offenders** (paragraph 6.44).

36 Information provided by the NDNAD Strategy Board detailing requests that it has received for research access to the NDNAD and stored samples is superficial. In many instances, it is unclear what the research proposal actually led to. Requests for research with 'commercial' purposes will require particular scrutiny from the NDNAD Strategy Board, to ensure that research that primarily supports the development of a business opportunity does not gain approval unless fulfilling strict criteria. It is not clear that such strict criteria are currently

applied. **At present, there is a significant lack of transparency concerning research using the NDNAD and stored samples, with the cursory details provided in the NDNAD Annual Report being inadequate. Given this lack of information, it is not possible for the public to be reassured that research projects will only be approved if their potential benefits are sufficient to outweigh the harm to the other interests involved. We recommend the regular publication of further details concerning, as a minimum:**

- **information on requests and approvals, including the criteria used to determine approval or refusal;**
- **whether there was informed consent for the use of biological samples;**
- **which individuals have been given approval to undertake research projects using the NDNAD and stored samples;**
- **exactly what the purpose of this research was;**
- **whether the research has been subject to adequate levels of scientific and ethical review; and**
- **the outcomes of research** (paragraph 6.25).

37 Analysis and storage of biological samples is currently performed by three companies (their number is set to rise). Given that biological samples may yield sensitive personal information, it is imperative that robust, internationally recognised regulations are in place that prohibit unlawful access to, and unlicensed transfer of, the samples. **We recommend that organisations and companies that have custody of biological samples complete a standard Material Transfer Agreement[2], subject to ethical review, that establishes the terms and conditions under which samples may be accessed and used by subsequent recipients** (paragraph 6.34).

38 The subject samples sent by the police to the private companies are accompanied by the individual's 'datacard', which contains the name of the person from whom the sample was taken, and their gender. The private providers of DNA analysis have all commented that they have no need of the 'datacards' sent to their laboratories with subject samples[3], and yet their possession of them creates the possibility that the security and confidentiality of samples could be compromised. **We recommend that datacards should not be provided to private companies. Non-coded identifying details (such as a name) should be removed from the sample as early as possible during the DNA analysis and storage process** (paragraph 6.36)**. Further, we would make it an absolute requirement that any NDNAD samples or data provided for research should be irreversibly anonymised (that is, neither the researchers nor the Custodian or any NDNAD staff should be able to relate any result to any named individual). A condition of the release of any biological sample to researchers should be that the researchers would not profile the DNA of any sample. It would be necessary to ensure that, even if the researchers were to do so, they would never be allowed to interrogate the NDNAD to identify the individual with that profile. If such safeguards could not be put in place for a research project, the project should not be permitted** (paragraph 6.32).

39 **Notwithstanding the fact that the operation of forensic databases falls outside the purview of the Human Tissue Act (2004), we recommend that all research projects involving biological samples collected for forensic use be subject to the same regime of scientific, ethical review and oversight that currently governs access to, and use of, other human**

2. A Material Transfer Agreement (MTA) is a contract that governs the transfer of tangible research materials between two organisations, when the recipient intends to use it for his or her own research purposes. The MTA defines the rights of the provider and the recipient with respect to the materials and any derivatives.

3. Samples are identifiable by means of a 'barcode'.

biological sample collections in the United Kingdom. This is particularly so in light of the fact that the samples are not sufficiently anonymised (with a link to the datacard still possible after archiving of the sample), and also because none of the individuals whose NDNAD samples are stored has given their consent for their samples to be used for specific research purposes (paragraph 6.31).

Governance and ethical oversight (Chapter 7)

40 The forensic analysis of DNA and the retention of biological samples demand the highest operating standards in terms of accountability, security, quality assurance and ethical standards. The potential uses and abuses of forensic databases are considerable. While both the NDNAD and IDENT1 are subject to the laws governing human rights and data protection, 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.

41 The functioning of IDENT1 may raise concerns surrounding the 'linkages' with not just the Police National Computer (PNC), but other biometric and informational databases in the future. At present, however, there is no independent official or body charged with oversight of this resource or such linkage processes. **In our view, IDENT1, like the NDNAD, must retain public confidence in its security, especially its protection from non-authorised access and in control of its uses. This confidence depends on ongoing scrutiny and systematic audit of its uses so that the public can be sure that data held in it are not misused or misrepresented. There should be regular public reports on the use, scrutiny and auditing of this database** (paragraph 7.9).

42 The NDNAD Custodian (a named individual who heads the NDNAD Custodian Unit within the National Policing Improvement Agency (NPIA)) is entrusted with maintaining and safeguarding the integrity of the NDNAD and developing policy. This involves overseeing delivery of NDNAD operations and the Standards of Performance for forensic science laboratories accredited to provide DNA analysis for the NDNAD. The Custodian is currently establishing an Ethics Group to advise the NDNAD Strategy Board. **We recommend the development of a clear ethics and governance framework for the operation of the Ethics Group in order to establish:**

- **its relationship with the NDNAD Strategic Board;**
- **its remit, whether this be to monitor and/or advise or otherwise;**
- **its responsibilities for reporting publicly and handling complaints;**
- **its powers; and**
- **how it is to maintain its independence.**

Further consideration should be given to broader ethical oversight and governance in respect of the umbrella role of the Forensic Science Regulator and other forensic databases, such as IDENT1 (paragraph 7.25)**.**

43 Upon a request from an individual who wishes to have their bioinformation removed from a police database, a Chief Constable has the discretion to remove profiles and samples from forensic databases. The operation of this discretion must be transparent and consistent, and not partisan or self-serving, if the police are to retain public trust and confidence in police handling of personal information. Yet, whilst the Association of Chief Police Officers of England Wales and Northern Ireland's (ACPO) guidelines on 'exceptional cases'[4] are intended to ensure consistency, there is no substantive guidance on how to determine if a case is exceptional. Decisions therefore risk being arbitrary and potentially unjust. **At present, the 'exceptional**

4. See paragraphs 7.33–7.36.

circumstances' criteria for removal of records from the NDNAD and other databases are too restrictive, and the Chief Constable's discretion too wide. If the current system remains and records are not automatically removed for those not convicted, in accordance with our earlier recommendations (paragraphs 10–12 and 20) we recommend that:

- **There should be public guidelines explaining how to apply to have records removed from police databases, and the grounds on which removal can be required.**
- **The police should be required to justify the need for retention in response to a request for removal of an individual's records (with a strong presumption in favour of removal in the case of minors, see paragraph 20).**
- **An independent body, along the lines of an administrative tribunal, should oversee requests from individuals to have their profiles removed from bioinformation databases. The tribunal would have to balance the rights of the individual against such factors as the seriousness of the offence, previous arrests, the outcome of the arrest, the likelihood of this individual re-offending, the danger to the public and any other special circumstances** (paragraph 7.37).

44 Although forensic biometric databases are not currently linked to each other in any sophisticated fashion, it is a stated aim for databases to be 'inter-operable' in the near future. The ethical implications of such databases could then be 'multiplied' by linking with other databases. The concerns, particularly about privacy, where access to one database may permit access to information across several databases, may be further compounded if linkage is envisaged between databases across different countries. **We recommend, on the basis of standard European data protection principles, a minimum set of safeguarding requirements to consider before allowing access to bioinformation databases to international law enforcement agencies, which would be:**

- **to ensure there is a sufficient level of data protection in all authorities/agencies that would receive information;**
- **to subject each request to adequate scrutiny as to merit and reasonableness and on a transparent basis;**
- **to agree the criteria for sharing data, for example only for the investigation of serious crimes or in special circumstances; and**
- **to share only as much information as is necessary to meet the request and only to those authorities or agencies which 'need to know'** (paragraph 7.42).

45 **In addition to the recommendations made in Chapter 6, we recommend, not only that there must be robust procedures for assessing applications for research access to the NDNAD and stored samples, but that there should also be a requirement to articulate publicly the basis upon which applications for any access to data stored on bioinformation databases will be considered and the precise purposes for which access will, and will not, be granted either to police or non-police agencies** (paragraph 7.32).

46 Exchanges of data internationally are currently made on a case-by-case basis, with no agreed framework for sharing data. Various initiatives are underway to facilitate exchanges while maintaining quality standards and adequate levels of protection for individual rights. There is no oversight body to monitor the international exchange of DNA profiles, or organisation that could make enquiries (and pursue complaints) on behalf of individuals whose data have been misused. There have also been recent proposals for a centralised database of fingerprints across the European Union, with an attendant obligation on each Member State to transfer details held by national police forces to a central authority.

47 The Prüm Treaty (2005) is a cooperation agreement for exchange of information between, currently, eleven European Union Member States.[5] It has been offered as a model for the entire European Union. The direct access provisions would not apply until the data protection elements of the Treaty have been adopted into national laws. **The threshold for holding DNA profiles on a forensic database is far lower in the United Kingdom than in any other Member State of the EU, and the proportion of the population included on the UK DNA Database is correspondingly far higher than in other EU countries. The Government should as a matter of urgency examine the implications of DNA exchanges for those on the UK NDNAD. The Government should insist on the inclusion in the Prüm Treaty of provisions to ensure that its operation is properly monitored. At the very least, the following is required:**

- **an obligation on national agencies to produce annual reports, including statistics, on the use of their powers under the Treaty; and**
- **an obligation on the European Commission to produce an overall evaluation of the operation of the Treaty, for submission to the European Council, the European Parliament and national parliaments, to see whether it needs amendment** (paragraph 7.52)**.**

48 The current regulatory structure for bioinformation databases is not on a statutory footing and the legislative framework surrounding the forensic use of bioinformation is piecemeal and patchy. The regulatory architecture of forensic services is also currently in a state of flux in the United Kingdom.

49 **We recommend that there should be a statutory basis for the regulation of forensic databases and retained biological samples. A regulatory framework should be established with a clear statement of purpose and specific powers of oversight delegated to an appropriate independent body or official. This should include oversight of research and other access requests, for example for further testing of samples or familial searching and inferring ethnicity. We are pleased to see the establishment of an Ethics Group by the Home Office, with a remit to oversee the running and uses of the NDNAD, but its specific functions and powers must be more clearly, and publicly, articulated. Moreover, we consider that a longer-term view is required that considers the future possibilities and challenges that may come with increased access and linkage involving a range of forensic databases** (paragraph 7.55).

50 Throughout the Report we draw attention to the difficulty in assessing the impact of increasing police powers because of the poor quality or absence of official statistics (or conflicting statistics: see paragraphs 4.51–4.52). Moreover, on many vital issues such as requests to conduct research on databases and/or samples or general access provisions to the NDNAD, there is an absence of protocols or guidance. **We recommend a far greater commitment to openness and transparency and a greater availability of documents to public scrutiny. Where public access is denied for reasons of security and the administration of justice, this should be fully explained and justified. Efforts to improve the generation of data and statistics are welcomed, as are apparent efforts to increase the publication of data. These moves are still in their early stages, and their continuation is strongly supported** (paragraph 7.57).

5. Austria, Belgium, France, Germany, Luxembourg, the Netherlands, Spain, Finland, Italy, Portugal and Slovenia.