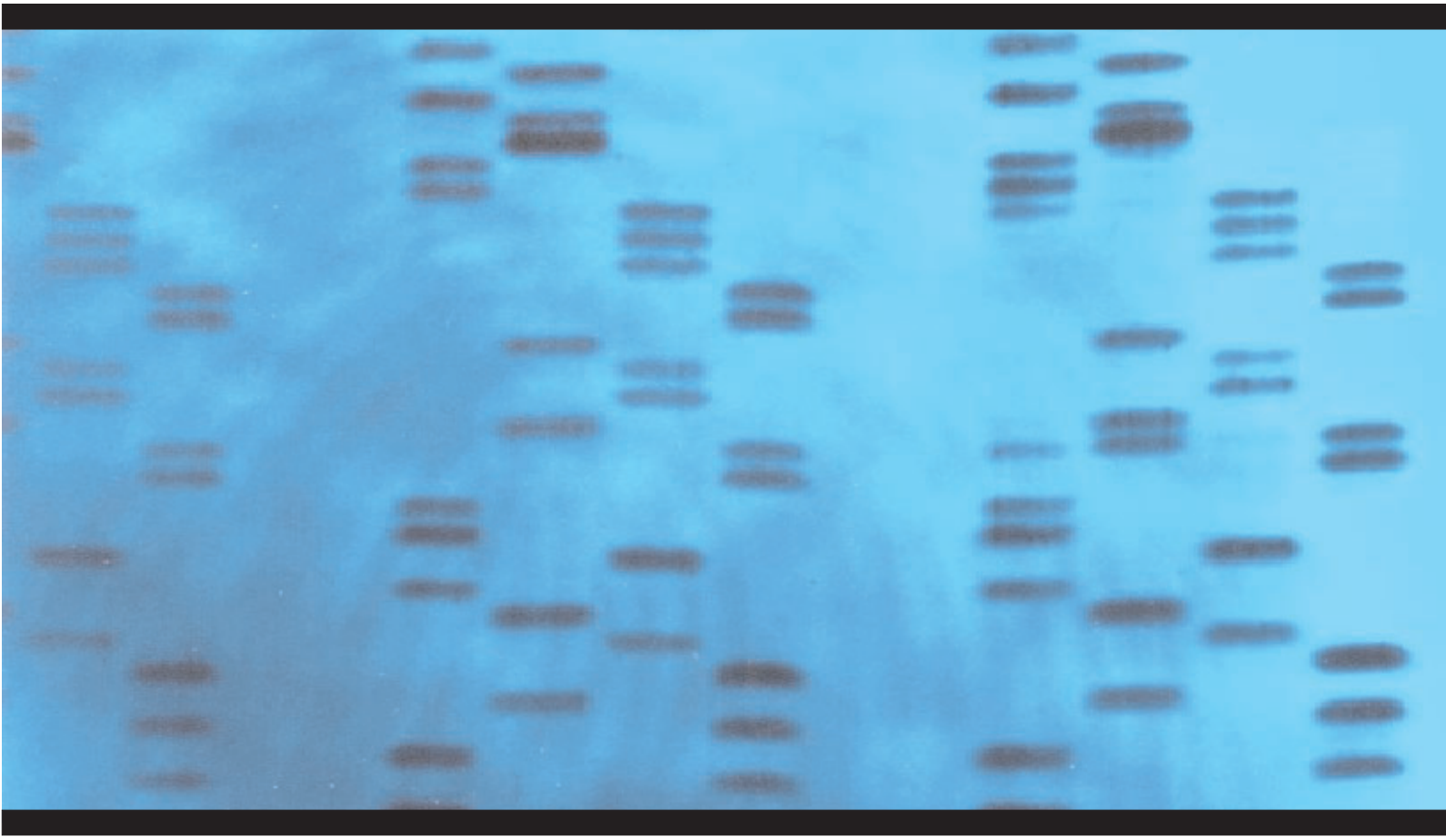
The Police National DNA Database:



Balancing Crime Detection, Human Rights and Privacy

A Report by GeneWatch UK

The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy.

A Report for GeneWatch UK by Kristina Staley

January 2005

The Mill House, Manchester Road, Tideswell, Buxton
Derbyshire, SK17 8LN, UK
Phone: 01287 871898 Fax: 01298 872531
E-mail: mail@genewatch.org
Website: www.genewatch.org

GeneWatch UK

Acknowledgements

GeneWatch would like to thank Jan van Aken, Sarah Sexton and Paul Johnson for their helpful comments on a draft of this report. Kristina Staley would also like to thank Val Sales for her help in preparing the report. The content of the final report remains the responsibility of GeneWatch UK.

Cover photograph

DNA genetic fingerprinting on fingerprint blue backdrop. © Adam Hart-Davis,
http://www.adam-hart-davis.org/

Contents

List of Boxes

1 Executive Summary

Using DNA to trace people who are suspected of committing a crime is one of the biggest advances in tackling crime since fingerprinting. When DNA profiling is used wisely it can bring major benefits to society by helping to convict serious criminals including murderers and rapists. Concerns arise, however, when tissue samples, genetic information and personal data are stored indefinitely on a DNA database, like the police forensic database known as the National DNA Database (NDNAD). There are fears that this information may be misused in ways that threaten our individual rights as well as those of our families. We must be confident that the police and the Government use DNA in a way that respects our fundamental right to privacy and protects our civil liberties.

The limits on police powers relating to the use of the NDNAD are enshrined in law. On 4 April 2004, these powers were extended. In England and Wales, the police are now allowed to take samples *without consent* from anyone who is simply arrested on suspicion of any recordable offence. This includes all but the most minor crimes. The new legislation also allows the police to keep this information indefinitely, even if the person arrested is *never charged*. This means the database now contains DNA profiles from 2.1 million individuals and is the most extensive DNA database in the world. No other police force has greater freedom to obtain, use and store genetic information from its citizens.

This report reviews the operation of the forensic DNA database in England and Wales, the benefits it may bring and the concerns that it raises. As the NDNAD continues to expand, GeneWatch UK believes there is a need for wider public debate on the use of forensic DNA and makes a number of recommendations for improvements in the retention and handling of genetic information by the police. We are also concerned about likely changes in the future, including suggestions that everyone's DNA profile should be added to the database, and the introduction of new technology that could expand the use of genetic information. GeneWatch UK hopes this report will encourage and inform society's deliberations on these difficult and sensitive subjects.

DNA in crime detection

The NDNAD is a database used by the police that contains DNA data held on a computer and stored samples from the scenes of crimes as well as from people who have been arrested, acquitted or convicted of a crime. The DNA from every sample is analysed in a limited number of areas to produce a 'DNA profile' for each individual or sample from the scene of a crime. The database relies on the fact that every person's DNA is unique (unless they are an identical twin) and that the chance of an identical match between the DNA sequence taken from two different people is very low – less than one in a billion if they are not related. However, it is possible to get 'false' matches and the chances of a 'false' match are increased (i.e. the wrong person is identified) if samples are obtained from people who are related or if the DNA profile is incomplete. Incomplete profiles are often obtained from scene of crime samples because the DNA is often degraded.

Following collection and analysis of a sample, a new DNA profile can be compared with the profiles stored on the database. A match can arise in four different ways. If:

1. a new scene of crime profile matches the profile of an individual already on the database. This can help to identify a potential suspect very rapidly;
2. a new individual's profile matches a stored scene of crime profile from an unsolved crime or crimes on the database. This type of 'speculative search' can identify a potential suspect long after a crime has been committed;

3. a new scene of crime profile is found to match that of an old crime scene. This can help the police in their investigations even if a suspect is not identified; and
4. the person has been sampled and included on the database previously under the same or a different name.

Therefore, DNA profiling is a powerful tool in solving many serious crimes and deterring serious criminals. In a typical month, matches are found linking suspects to 30 murders, 45 rapes and 3,200 motor vehicle, property and drug crimes.

Concerns about the use of DNA profiling and the National DNA Database

There are concerns about the use of this technology since DNA is very different from other types of forensic data – it has the capacity to reveal a lot more personal information. For example, DNA data may reveal whether a person is at risk of ill-health as well as who they are related to. Giving the police or state access to DNA data and samples can therefore give them much more information about a person than simply who that person is.

The major concerns about the use of the NDNAD relate to:

Balancing the rights of individuals and the interests of society

Society has an interest in reducing crime. Most people want criminals to be caught, detained if necessary and, if possible, rehabilitated so they do not commit further offences. A temporary removal of some rights is widely agreed to be a reasonable punishment for committing a serious crime. But current use of the NDNAD has the potential to threaten the individual's right to privacy and civil liberties much more widely.

The biggest threat to people's right to privacy is posed by the indefinite retention of DNA samples, because these could provide unlimited amounts of genetic information about known individuals. The usefulness of retaining samples after the DNA has been analysed is questionable, even in the case of convicted criminals. If a person is found to be innocent, there does not seem to be any compelling reason why their sample should be retained and their rights to privacy should be denied. The law in England and Wales is unique in allowing samples from large numbers of innocent people to be retained indefinitely.

The NDNAD also threatens our civil liberties because of its potential to be used as an instrument of surveillance. Expanding the database puts increasing numbers of people on a permanent 'list of suspects' even though they may never have been charged or convicted of a crime. This may subtly alter the way they are viewed both by the state and by their fellow citizens, potentially undermining the principles of 'innocent until proven guilty' and of rehabilitation. The NDNAD is also the only database that keeps a person's 'criminal' record indefinitely, no matter how trivial their offence. This raises the concern that records on the NDNAD could be used in future to restrict people's rights and freedoms, for example to make it difficult for them to obtain employment.

The increasing threats to our 'genetic privacy'

The current DNA data used for identification purposes contains very limited information about a person's genes. However, this may change in the future with plans to use new technology to exploit the information in DNA samples. Some advocates have argued that this technology will be able to predict the characteristics of a suspect from the DNA evidence at the scene of a crime, generating a description along the lines of 'a tall man, with red hair, blue eyes, who's probably overweight'. Researchers are also looking at predicting ethnicity and health status. Some even believe it will be possible to predict a person's personality or behaviour. However, there are serious scientific problems with most of these approaches. Not only is some of the research fundamentally flawed, much of it is unlikely to produce particularly useful or accurate predictions. There is also a danger that the information will be used selectively to reinforce

existing prejudices, for example about race or skin colour. Nevertheless, a few genetic tests can reveal important information about some people's health. If use of this new technology were expanded to stored samples from known individuals on the database, the increase in police access to genetic information could pose an even greater threat to privacy.

A lack of transparent mechanisms of governance and oversight

Some uses of the NDNAD are particularly controversial or sensitive. For example, familial searches can be used to trace suspects if they have any relatives on the database. Such an investigation can represent a major intrusion into family life. There is a risk it may uncover family relationships that people do not know about, including cases of non-paternity. However, as yet there are no guidelines as to when such an approach can be considered ethical and what the implications might be for data protection. This situation is inadequate and open to abuse.

Similarly, researchers using the NDNAD do not have to seek consent from participants or the approval of an independent ethics committee to carry out their research. They have only to seek permission from the NDNAD Board. Some of the research could be highly controversial, for example research on ethnicity and criminal behaviour. There is no guarantee that such controversial projects might not be undertaken in the future. The main organisation currently carrying out forensic research, the Forensic Science Service, is also heavily represented on the NDNAD Board. This creates an unacceptable conflict of interest.

Increasing police and Government access to personal data

Other national databases are being planned and developed, including the National Identity Register to support the use of ID cards, and the new NHS Electronic Care Record Service, which may contain some genetic data in the future. It is not clear under what circumstances the police will be allowed access to this information. Nor is it clear whether any of these databases will be linked, possibly allowing other Government bodies to find out who is on the NDNAD. Expanding and/or linking these databases would give the state unprecedented abilities to monitor the UK population, greatly increasing the threats to our privacy. There are concerns that this access could all too easily be abused, taking the UK closer towards an oppressive 'police state'.

Errors in DNA profiling

There is no such thing as an error-free database. Mistakes can lead to 'false positives' where an innocent person is wrongly identified. A 'trawl of the database' is not enough to secure a conviction in court: a fresh sample from the accused and corroborating evidence is also needed. But in some cases DNA evidence can be difficult to interpret, particularly when samples from the crime scene are degraded or contain more than one person's DNA. Currently, the criminal justice system may not always take sufficient account of the possibility of errors and people may be wrongly convicted either by mistake or even by being 'framed'.

Recommendations –getting the balance right

At GeneWatch UK, we recognise the benefits of the NDNAD but we also believe that its current operation does not strike an appropriate balance between the rights of the individual and the interests of the public. While there is no doubt that society does have an interest in the detection and prevention of crime, this cannot be used to justify every infringement of the individual's right to privacy and the loss of our civil liberties. This is especially true for people who are innocent. In this regard, we believe the UK needs to bring its criminal justice legislation more in line with the rest of Europe. There are changes that could be made to the operation of the NDNAD which would protect people's rights and increase public confidence without compromising its role in fighting crime.

Recommendation 1: DNA samples (except samples from the scene of a crime) should not be retained once an investigation is complete. Only DNA profiles and personal data need to be on the database to find a 'match' for a criminal investigation. Research uses of the database itself (profiles and personal data) should be restricted to producing 'quality control' statistics on the type of data that has been added and how the data is being used.

This recommendation removes concerns that samples could be used for purposes other than identification, such as research into criminal behaviour, without the individual's consent. Suspects' samples need to be retained for a certain length of time so they can be analysed and the profiles can be checked. However, destroying the sample once an investigation is complete does not in any way restrict future searches for matches. All the information that is needed is stored in the DNA profile held on a computer. Physical samples do not need to be retained to prevent errors because a fresh sample must be taken anyway before DNA evidence can be used in court. Although it can be argued that samples may need to be reanalysed if the technology is updated, in reality upgrading the DNA profiling system used on the database seems to be both costly and unnecessary.

The right to consent or refuse to take part in research is an important right for individuals and for society. It is not necessary to use samples or profiles taken without consent to do legitimate genetic research. It is also questionable whether the NDNAD provides a robust source of data. Categories within the database such as 'ethnic appearance' are meaningless for scientific purposes and the DNA profiles and samples will not be representative of either the general or the 'criminal' population. Genetic research using the database is therefore likely to be misleading as well as controversial.

Recommendation 2: An independent body should be set up to review all future applications to access the data and samples for forensic and non-forensic purposes; to ensure standards are maintained; and to ensure public accountability and transparency.

We are concerned both about the current use of the NDNAD and the potential for the increased threats to privacy in the future. We think it is essential that the NDNAD is made more accountable to the public. We therefore believe that a new independent body should be created that includes lay representation. This body should be made responsible for deciding when 'familial searching' is allowed, rather than leaving this decision to the police alone.

This body should also review the merits of methods which attempt to predict the characteristics of individuals from DNA samples left at the scene of a crime. There is a danger that attempts to predict physical appearance, or other characteristics, may hinder rather than help investigations by providing producing misleading information.

Recommendation 3: An 'Innocence Project' should be established to investigate possible miscarriages of justice using DNA.

DNA profiling can be a powerful tool to help establish innocence as well as guilt. DNA evidence can also be misinterpreted and lead to miscarriages of justice. A project like the US 'Innocence Project' could help increase public confidence that DNA profiling is being used wisely to improve the criminal justice system in England and Wales. The current system does not assist in reviews of cases where there is reason to suppose people have been wrongly convicted.

Recommendation 4: An independent review of whose DNA data should be sampled and retained is urgently needed. Research on the use of the NDNAD, its effectiveness and the justification for including innocent people, should be conducted to inform the debate.

Like others, we are concerned that the legislative changes to date have been introduced too rapidly and in the absence of any meaningful public debate. We believe that further

deliberation is needed to find out what the public would accept as a reasonable balance between protecting the right to privacy and protecting citizens from crime. The public should have a say as to whose data is included on the database and for how long.

There is no data available to evaluate whether crime detection will be improved by including DNA profiles from people who are arrested and not charged, or by continuing to hold data on people whose charges are later dropped or who are found to be innocent. GeneWatch UK's current view is that:

The personal data and DNA profiles from people whose charges have been dropped, or who have been acquitted, should be removed from the NDNAD (unless they were connected with a serious violent or sexual offence). During the investigation stage, it will have been possible to check whether their profiles match those from any crime scene on the database. Keeping innocent people on the database effectively means treating them as criminals. This undermines the principle of 'innocent until proven guilty' and is open to abuse, particularly in relation to 'political' offences involving peaceful protest. Making this change would also bring the NDNAD more in line with record-keeping on the Police National Computer.

DNA samples should not be taken until a person has been charged, **unless needed to help prove or disprove a suspect's involvement in a *specific* offence**. The process of charging someone with an offence is more formal than simply making an arrest. Waiting until a person has been charged reduces the risk that speculative searching for matches using the database is arbitrary and unfair or that someone could be 'framed'. This is an important safeguard to prevent the database being used in a discriminatory way.

The database should *not* be expanded to include the whole population. Threats to privacy and civil rights are more likely to be increased than reduced by proposals to expand the database; it would not prevent the database from being used in a discriminatory way and would only serve to increase the potential for state surveillance. In addition, in the case of a larger database, the probability of false matches and the resources needed to investigate each match could increase disproportionately to the number of solved crimes.

People's personal data and DNA profiles should not be kept indefinitely on the database (except when they have committed serious violent or sexual crimes). Keeping records indefinitely raises concerns about civil liberties, particularly when offences are related to peaceful protest or political dissent. This practice also undermines the principle of rehabilitation. Records on the Police National Computer are removed after a certain length of time, depending on the seriousness of the offence. Records for serious, violent and sexual offences are kept indefinitely, but most other records are eventually removed. A similar system of restrictions on retention should apply to the NDNAD.

2 Introduction

This report is concerned with the potential threats to privacy and civil liberties posed by the police use of the National DNA Database (NDNAD) and how these are balanced against the benefits of using DNA in criminal investigations.

The report provides a brief introduction to the NDNAD and the different ways that the police use DNA evidence. The details of how DNA samples are obtained, processed and stored are provided as well as information about how this intelligence is used to trace suspects. The limitations of the technology, the different sources of error and the need for this evidence to be used with caution are also discussed in depth.

The report goes on to consider the limits to police powers around the use of the NDNAD as described in law. Current legislation in England and Wales is compared to that of other European countries and the United States to explain how the permissive legislation in England and Wales has enabled the creation of one of the biggest forensic databases in the world.

The future of forensic DNA profiling is also considered, particularly the proposed changes to the technology and the use of genetic data to predict a suspect's characteristics. The policy developments likely to impact on police use of the NDNAD and other databases in the future are considered, including potential threats to privacy and civil liberties.

Finally, the limitations of existing laws and safeguards are discussed and the steps that could be taken to give greater protection to our rights and freedoms are identified.

3 What is the National DNA Database?

The UK National DNA Database (NDNAD) is a police intelligence database that uses DNA to identify criminal suspects and to find links between different crimes.[1] It was set up in April 1995 by the Forensic Science Service (FSS) which has since become a world expert in the use of forensic DNA technology.

The NDNAD relies on the fact that DNA can be obtained from any sample of human tissue left at the scene of a crime (SOC).[2] This is not just limited to violent crimes where the offender leaves a sample of blood or semen; the technology is now so sensitive that genetic information can be extracted from minute samples such as a fingerprint left on a door handle, or the saliva left on a cup or a cigarette. The extended use of the technology now means that the NDNAD contains information from a wide range of crimes. Data from every new crime scene is routinely analysed to see if it matches a known individual on the database or any other SOC sample. This not only helps to identify suspects, but can also help prove that a person is innocent.

In March 2004, the FSS reported that:[3]

> The NDNAD contained DNA profiles from around 2.1 million individuals and 215,000 crime scenes.
>
> In a typical month, matches were found linking suspects to 30 murders, 45 rapes and 3,200 motor vehicle, property and drug crimes.
>
> When information from a new crime scene was added to the database, there was a 40% chance of an immediate match between the scene of crime (SOC) sample and a known individual.
>
> The total value of Government investment in the NDNAD up until that point had been £182 million, and that a further £61 million was going to be invested in the following year to support a major expansion of the programme.

The limits on police powers relating to the use of the NDNAD are enshrined in law. On 4 April 2004, these powers were extended. In England and Wales, the police are now allowed to take samples without consent from anyone who is arrested on suspicion of any recordable offence. This includes all but the most trivial crimes. The new legislation also allows the police to keep this information indefinitely, even if the person arrested is never charged. This means the database is the most extensive in the world and is predicted to expand to include around 5 million people (about 10% of the population).[4]

3.1 Using DNA to identify individuals

DNA (deoxyribonucleic acid) is found in every cell in the body. It is passed on from one generation to the next. Half our DNA is inherited from our mother and half from our father. Except for identical twins, every single person's DNA is unique. DNA can therefore be used to try to identify an individual in a similar way to a fingerprint.

However, DNA is very different from other types of forensic data because it has the potential to reveal a lot more information about a person.[5-7] Unlike a fingerprint, DNA can:

- potentially provide some hints about what a person looks like;
- potentially indicate whether a person is at *risk* of developing an illness in the future or has a rare genetic condition;
- reveal who a person is related to – if your DNA is held on the NDNAD it could be used to trace your brothers, sisters, parents or children.

Giving the police access to DNA samples therefore provides them with a lot more information than a fingerprint does, potentially including personal information about health and relationships.

3.2 How the police use DNA

If the police obtain a DNA sample from a crime scene there are several ways they can use this information to find out who it came from:

If there are already one or more known suspects for the crime the police can take DNA samples from all of them to see if they match the scene of crime (SOC) sample.

If the police suspect that the person who committed the crime lives in a particular village or works at a particular place, they can ask everyone in that village or workplace to give a DNA sample in order to try to find a match. These mass screenings can also help to eliminate a lot of people from police enquiries.

The police can compare the DNA obtained from the crime scene with information on the NDNAD. If they find a match, the database will give them details about the person they are trying to find. If they do not find an exact match, they may still be able to identify relatives of the person they are looking for.

The police can go to court and ask for permission to search other DNA databases for a match (for example, databases collected for health research), if they can convince the court that this is in the public interest.

The police can use new techniques to see if the genetic information in the DNA sample can give some clues about the person they are looking for, such as their hair or skin colour or their state of health although these techniques currently have serious limitations. Some researchers claim that it might also be possible in future to predict certain aspects of behaviour from a person's DNA (such as a tendency to aggression or addiction) but this is much more controversial.

3.3 Concerns about police use of DNA – our right to privacy

Analysis of DNA can be a powerful tool to help solve crimes. Using DNA evidence wisely can bring significant benefits to society by helping to convict murderers and rapists. Few people have problems with the idea of the police comparing the DNA of a suspect with DNA left at the scene of a serious crime, provided this evidence is used carefully when a case comes to court. However, concerns arise when tissue samples, genetic information and other types of personal data are stored on a DNA database. There are fears that this information may be misused in ways that threaten our individual rights as well as those of our families especially our right to privacy. Even the police have some concerns about the implications of DNA databases for their own privacy (see Box T).

Privacy as a right

Privacy is a fundamental human right. A UK legal committee has defined it as:[8]

'*The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information*.'

In a free and democratic society, respect for privacy sets an essential limit on the power of both the state and private organisations to intrude into people's lives. The importance of protecting privacy is recognised by many international and national treaties including the Universal Declaration of Human Rights[9] and the European Convention on Human Rights, which has recently been adopted into UK law.[8]

The collection and storage of personal and genetic information by the police is viewed as a threat to our '*information privacy'*.[10] Human genetic data is widely recognised to have special status because of its ability to reveal private information about a person's health and family relationships.[11] It is therefore argued that all DNA databases, including those held by the police, deserve special measures of protection. There is also a more general concern that the other personal data on the NDNAD (and other national databases see Section 8) could support an increase in population surveillance, taking us closer towards an oppressive 'police state'.

These fears are not unfounded. Within living memory, both fascist and communist governments in Europe have used identity papers and other personal records as a means of oppressing different populations. Rights and freedoms need protection because:

1. they are hard to win and easy to lose;
2. some people may be particularly vulnerable to erosion of their rights, including people who use mental health services or people from ethnic minorities.

Balancing the interests of the individual and the state

When someone is suspected or convicted of a crime, their rights are restricted in ways that depend on the seriousness of the offence. Before someone is convicted, there are strict limits as to how far their rights can be removed. These limits are designed to allow the police to do their job without giving them so much power that they can act in an arbitrary or unjust way. If the person is subsequently acquitted, they can then expect to be treated like any other citizen. This prevents false accusations from seriously damaging people's lives. If the person is subsequently convicted of a serious offence, they can then expect to be sent to prison and to lose some of their rights to freedom and privacy.

It is not clear that the police use of DNA databases represents a 'fair and just' restriction of our right to privacy. The NDNAD contains information about people convicted of a wide range of offences; people arrested but never charged; people who have been acquitted; and people who have given their samples voluntarily. They all face the same threats to their rights. The biggest concern is that the police or Government could use 'the pursuit of criminal justice' to defend any use of people's personal or genetic information without their knowledge or consent. There is a danger that the balance of interests between the individual and the state may end up going too far in one direction (also see Section 9).

4 What Information is Stored on the NDNAD? How is this Information Obtained?

The National DNA Database (NDNAD) contains genetic information in the form of DNA profiles from both potential suspects and different crime scenes. It also contains more routine information about people, for example their name and sex. An Arrest Summons Number allows information on the NDNAD to be linked with information on the Police National Computer (PNC). The PNC consists of linked databases holding extensive data on criminals, vehicles and property (see Box O). A barcode reference number also allows information on the NDNAD to be linked with the corresponding DNA sample, which is kept frozen in storage.

Police forces supply the DNA samples used to derive the DNA profiles on the database, but individual police officers do not access the NDNAD. The Forensic Science Service (FSS) owns and manages the database for the Association of Chief Police Officers (ACPO) and supplies the police with information about matches between DNA profiles.

The details of how this information is obtained and stored are described below.

4.1 DNA profiles

It is useful to know something about the science and technology involved in DNA profiling in order to understand the strengths and weaknesses of DNA analysis as a tool for crime investigation.

The technology used to obtain the data for the NDNAD does not examine every single difference between people's DNA. It is restricted to looking at specific areas known as short tandem repeats (STRs) (see Box A).[1] STRs are places in the DNA where a short section of the genetic code repeats itself. People have varying numbers of repeats, which is how STRs can be used to identify individuals.

Ten different STRs are analysed in each DNA sample. Because each STR is made up of two strands – one from the person's mother and one from their father this analysis produces 20 bits of information.[12] The DNA profile then simply consists of a string of numbers indicating the exact number of repeats at each of the ten STRs plus information about the person's sex. People may have the same number of repeats at any one STR, but it's the information from all ten that gives each person their individual profile.

The STRs analysed for DNA profiling are located in non-coding sections of DNA. These are parts of the DNA that do not contain any instructions for making proteins or any other cell product. This means they are not part of genes and are not thought to be important in influencing biological differences such as health or appearance. Therefore, the DNA profiles themselves are thought to contain very limited amounts of genetic information.

When all the numbers in two complete DNA profiles match exactly, forensic scientists can be very confident that they come from the same person (except in the case of identical twins).[14] The probability of full DNA profiles from two unrelated people matching just by chance is very low, less than one in a billion.[12] However, the chances of a 'false' match are increased (i.e. the wrong person is identified) if samples are obtained from people who are related; or if the DNA profile is incomplete. Incomplete profiles are often obtained from SOC samples because the DNA is often degraded.[1] This is one important reason why DNA profiling is not foolproof (see Section 5.2).

BOX A: Analysing short tandem repeats (STRs) to generate a DNA profile

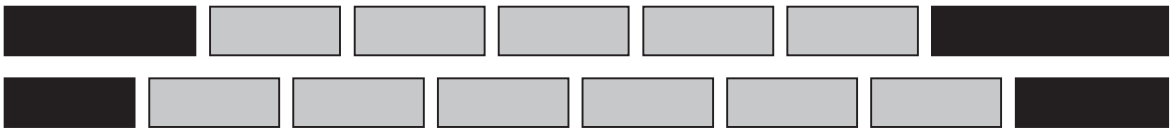


Diagram of a single STR. We have two copies of each repeat region, one inherited from our mother and one from our father. The repeated sequence in STRs is typically twoseven base pairs in length. (A base pair is formed by the connections between two nucleotides on opposite strands of the DNA. It is equivalent to 'one rung' on the 'DNA ladder'.) The number of times it is repeated usually varies between seven and 30.[13] The short length of the STRs makes it possible to amplify these sections of DNA using a laboratory technique known as PCR.[2;14] This also makes it possible to obtain DNA profiles from very small samples and from old samples where the DNA may have degraded.

The end result of DNA profiling is a set of two numbers showing the number of repeats in each of the ten STRs. In the simplified diagram above this would be '5 6'. A complete profile would include all 20 STRs and information about gender. A gene called amelogenin is used for finding out the sex of a sample. Males have X and Y versions; females have only the X version because they inherit two copies of the X chromosome. So the final DNA profile of a man would look something like:[15]

17 17; 14 17; 11 12; 16 17; XY; 13 14; 30 31; 11 23; 14 15; 7 8; 21 23.
The first STR technique, introduced in 1994, looked at only four STRs. The next development, using SGM (second generation multiplex) profiling, looked at six STRs and the present-day technology, known as SGM Plus™ , looks at ten STRs. Using a greater number of STRs increases the discriminatory power of the test, reducing the number of 'false' matches.[1]

4.2 Obtaining a DNA profile from a tissue sample

The police are responsible for collecting all tissue samples, which they now do routinely as part of their investigations. Special kits are provided for this purpose: one for obtaining samples from individuals who have been arrested, known as criminal justice (CJ) samples; one for taking samples in a mass screening; and one for scene of crime (SOC) samples. There is also a kit for taking samples from individuals for use as evidence in court; these are known as case work (CW) samples. Each kit has a unique barcode to allow the sample to be traced accurately through the system. The process of obtaining a DNA profile from a tissue sample is described below.

Obtaining a DNA profile from an individual's sample (a CJ sample)[16;17]

- The process usually begins at a police station when an officer takes a tissue sample from a newly arrested person. The police first check the Police National Computer (PNC) to see if the individual's DNA profile is already on the NDNAD a fresh sample is not taken if an existing profile is confirmed.[18] Most often a sample is obtained via a mouth swab a large cotton wool bud is rubbed inside the suspect's cheek to loosen and collect skin cells. Alternatively, ten hairs with roots can be removed from the head.
- The sample is then put into a small plastic tube which is sealed. The process is repeated so that there are two samples for each suspect.
- The police keep their own record of who has given a sample on the PNC database. Each police record is given an Arrest Summons Number (ASN).

- The sample tubes are labelled with a unique barcode sticker. These are then placed into a special tamper-proof, clear plastic bag. The bag also contains a card with the same barcode label and other written details such as the type of alleged crime; the date the sample was taken; the suspect's name and age; and the name, number and rank of the officer taking the sample.
- The bag is sealed and the samples sent to an accredited DNA profiling laboratory for processing. There are currently five organisations that are approved to supply DNA profiles to the NDNAD: three public laboratories (the FSS and the Strathclyde and Tayside Police laboratories in Scotland); and two private companies (Cellmark and LGC Limited).
- Staff at the sample reception unit check the integrity of the tamper-proof bag before it is opened and the card is also checked to ensure all the details have been filled in. A scanner is used to record the details of each sample onto the computer system.
- One of the two submitted samples from each individual is kept frozen in storage by the laboratory that carries out the analysis. This 'back up' sample will be kept until the person would have reached the age 100 if no further information is obtained about them. However, if it's confirmed that someone has died, the sample will only be kept for one more year before it is destroyed.
- The other sample is processed to obtain a DNA profile. The DNA is first extracted from the tissue. It is then amplified in a heating and cooling process that creates millions of copies of the original DNA – like a biological photocopier. The technical term for this process is the polymerase chain reaction (PCR).
- The amplified DNA sample is separated out into the 11 specific areas that make up the profile (ten STRs and the sex marker). A laser detector is used to detect and record the presence of different DNA fragments distinguished by their size (see Box A).
- The data is analysed by computer which assigns numbers relating to the number of repeats in each of the STRs. This produces a string of numbers for loading onto the NDNAD.
- The DNA profile is sent by computer to the Forensic Science Service (FSS) to load onto the NDNAD as part of a new criminal justice (CJ) record. Each CJ record contains the following information:
  - the unique barcode reference number (which provides a link to the stored DNA sample)
  - the Arrest Summons Number (which provides a link to the record on the PNC)
  - the person's name
  - their date of birth
  - their ethnic appearance
  - their sex
  - information about the police force that collected the sample
  - information about the laboratory that analysed the sample
  - the sample type (blood, semen, saliva etc.)
  - the test type
  - the DNA profile.

Obtaining a DNA profile from a scene of crime (SOC) sample[16]

The police collect a variety of evidence from crime scenes in the hope of obtaining a DNA profile from the perpetrator. This includes samples of blood, semen, hair and urine as well as saliva from cigarette butts, drinking glasses, stamps, envelopes, chewing gum etc.[19] The sensitivity of the tests has increased to point where even brief contact with a mobile phone, computer keyboard or steering wheel can leave sufficient material to generate a DNA profile.[20]

Scene of crime (SOC) samples go through the same set of processing steps as CJ samples. However, because DNA can be broken down by heat, moisture and sunlight, the DNA in SOC samples is often degraded and the profiles often incomplete. An SOC profile must contain a minimum of eight STRs for it to be loaded onto the NDNAD, although one-off searches can be made with profiles containing only six STRs.

Each SOC record contains the following information:

- the unique barcode reference number
- information about the crime
- information about the police force that collected the sample
- information about the laboratory that analysed the sample
- the sample type (blood, semen, saliva etc.)
- the test type
- the DNA profile.

Who owns the data and the samples?

The data and the samples held in storage are the property of the police force that originally collected the sample and sent it to be analysed.[21] The FSS owns only the software and IT used to interpret the DNA profiles. It effectively provides a service for the police force, which has to pay for the analysis to be carried out.

5 How is the NDNAD Used to Identify Suspects? How Reliable is DNA Evidence?

5.1 Using the NDNAD to identify suspects

Once new criminal justice (CJ) profiles and DNA profiles from crime scenes (SOC profiles) have been loaded onto the NDNAD, the computer analyses the results overnight, comparing new profiles with those already on the database.[16] The following morning, 'match' reports are printed out. There are four types of matches revealing links between:

1. a new SOC profile and the CJ profiles of individuals already on the database. These matches can identify potential suspects very rapidly.
2. a new CJ profile and the stored SOC profiles from unsolved crimes on the database. This type of 'speculative search' can identify suspects long after the crime has been committed.
3. two or more unsolved crimes, when a new SOC profile is found to match that of an old crime scene, although the identity of the perpetrator is not revealed.
4. a new CJ profile and a CJ profile already on the database, suggesting that the individual has already been included on the database, under the same or a different name.

Information about matches is sent to the relevant police force purely as *intelligence information* (this initial information is not used in court). The police use this data to assist their follow-up investigations. A match is by no means proof that someone is responsible for a crime. The DNA evidence can show only that someone has probably been present at the crime scene.[19] The person may well have been there, but not at the time of the incident. It is up to the police to find all the additional supporting evidence to prove that someone is guilty (see Section 5.3).

Finding suspects via their relatives

Familial searches allow the police to identify a suspect even if their profile is not on the NDNAD by looking for partial matches between SOC profiles and the profiles of people who might be closely related.[1] The searching process produces a long list of names. Every one of them has to be contacted by the police to see whether they have a relative who could have possibly committed the crime.

This approach has been used successfully in a small number of cases (see Box B).[1] However, it is more controversial because it clearly represents a major intrusion into family life – there's a risk it may uncover family relationships which people do not know about. For example, the evidence from the 'familial search' might suggest that several people on the database are related to each other and to the unknown suspect for the crime. But, prior to being contacted by the police, some of these people may not know who their genetic father is – and may believe that they are part of an entirely different family.

BOX B: Use of familial searches to find suspects

Case 1: Teenagers Pauline Floyd, Geraldine Hughes and Sandra Newton, all from south Wales, were raped and strangled in 1973.[1] Despite a huge hunt for the murderer at the time, the cases remained unsolved for more than 29 years. In November 2000, the FSS used DNA profiling to analyse stains from the clothing of two of the girls but failed to find a match on the NDNAD. In 2002, DNA profiling was used to test items from the scene of the third girl's murder and links between the three crimes were revealed for the first time. Again the NDNAD failed to provide a suspect. Therefore a familial search was adopted to try to find people on the database who might be related to the perpetrator. The search yielded fewer than 100 names. In combination with the intelligence already available, this new information led to a local man, Joseph Kappen, being identified as the prime suspect. But Kappen had already died, so a proxy DNA profile was created by analysing samples from his family members who had volunteered to help with the investigation. The results of these tests confirmed that Kappen's profile was very likely to be a match, which led to his body being exhumed. Subsequent DNA analysis of his remains showed a perfect match with the SOC samples from all three murders.

Case 2: Craig Harman was the first man to be convicted in Britain following the use of a link between DNA retrieved at the scene of a crime and the DNA profile of a relative.[22] In March 2003, Harman dropped a brick from a footbridge above the M3, which then smashed through the windscreen of a passing lorry. The driver, Mr Little, suffered a heart attack after the brick hit him in the chest, and he died. DNA evidence was obtained from fingerprints left on the brick. A subsequent search of the NDNAD did not produce a match, but did identify a number of people with similar profiles, including a relative of Mr Harman. It was this crucial piece of evidence that helped to solve the crime. The match with his relative's DNA helped the police to identify Mr Harman as a potential suspect. A separate match between his own DNA and the DNA left on the brick was used as part of the evidence in court.

5.2 DNA profiling is not foolproof

In the case of DNA profiling, as with any other process that relies on *people* to carry out actions or make judgements, there is always room for mistakes. These can result in a number of different problems: the DNA profile may be incorrect although attributed to the right person; or the profile might be correct but attributed to the wrong person. This can lead to 'false' matches (or 'false positives') where an innocent person is wrongly accused of a crime. Alternatively it can lead to 'false negatives' where a criminal escapes detection and is then able to reoffend.[2;23-26]

The possibility of errors therefore undermines the usefulness of the database and the reliability of DNA evidence.[27] The size of such errors is hard to calculate and is still under dispute.[28;29] However, the errors are certainly not negligible and do need to be taken into consideration. The different sources of error and the steps being taken by the NDNAD to minimise their impact are described below:

(a) Contamination of samples

DNA samples can become contaminated if they come into contact with DNA from another person. This contamination results in a DNA profile containing information from an 'outsider'. This can happen if a sample is mishandled by the police collecting the evidence or the laboratory staff carrying out the analysis. It is easier to detect in CJ samples because these should contain only a single profile. It is more difficult in the case of SOC samples, because these are quite likely to contain DNA from more than one person. Even trace amounts of outsider DNA can complicate the analysis, so the contamination of samples can lead to serious problems.[13;24] (See section (c) below.)

What measures are taken to reduce the risk of contamination?

Since the whole process is critically dependent on collecting high-quality uncontaminated samples from crime scenes,[13] trained Crime Scene Examiners (CSEs) are employed by police forces as experts in sample collection. Both the police and the CSEs are required to take precautionary steps to avoid contamination. These steps include controlling access to the crime scene; wearing gloves and face masks; and carefully packaging, sealing and labelling evidence.[18]

At the processing stage, laboratories use controls and checks to assess the quality of DNA profiles and to check for contamination. When a problem is picked up, the sample can sometimes be reanalysed to produce a valid result. Additional tests can also eliminate profiles from laboratory staff and the police.[12] Elimination databases have been set up specifically for this purpose. These are searched only at the request of a senior officer if they are concerned that contamination has taken place.

If the source of the contamination is not known or cannot be eliminated, then the result is considered invalid and the data is not added to the NDNAD. However, it is not clear that all contaminated samples will be identified.

(b) Poor practice – errors in data handling

These types of error occur when samples are mislabelled during processing or when data is not entered correctly onto the computer.[1] Inevitably, there are always going to be these kinds of mistakes, but it is important that they do not arise out of sloppy practice. In the USA, forensic laboratories have been found to routinely mishandle samples and follow incorrect procedures (see Box C).

BOX C: Poor practice in US police laboratories leads to wrongful convictions

Problems in US police laboratories began in spring 2001,[30] when a lab worker realised that her colleague had not been using the correct procedures to eliminate police DNA profiles from samples from the scenes of crimes. More than 100 DNA tests were called into question. The first sample to be retested in Houston, Texas, showed that the DNA profile used to convict a man serving 25 years for rape could not possibly have been his.[31] The FBI played down the problem, claiming that it was an 'isolated incident' and that it should not undermine public confidence in its labs. It also announced that it would invest an additional $1 billion in the US national database to both expand its use and to provide greater quality assurance.

What measures are taken to reduce the risk of errors in data handling?

In practical terms, new automated systems are being developed to reduce the number of times that people have to handle the samples and so reduce the risk of human error.[14;32] But crucially the reliability of the results still depends on the people doing the testing. They are therefore required to go through a regular series of checks. These are overseen by the FSS's Custodian of the NDNAD and take the form of: [1;12;21]

Accreditation: The laboratories that carry out the DNA analysis have to pass a proficiency test before they are allowed to put profiles on the database. They have to prove they can consistently produce DNA profiles that are reliable and compatible with those provided by other suppliers.

Performance monitoring: The laboratories have to prove that they are continuing to meet the required standards through a programme of internal and external quality audit. They have to repeat the analysis of 5 to 10% of the samples to show they get consistent results and demonstrate that they can maintain an error rate below 0.05% (i.e. no more than one error in every 2,000 samples analysed).

Audit and assurance: The Custodian and the team are also subjected to regular independent audits to ensure they are maintaining both the IT infrastructure and the quality of the data, as well as managing the flow of information between the central database, the forensic labs and the police.

(c) Misinterpreting DNA profiles

DNA profiles may not always be complete. This is because, as samples age, DNA begins to break down. This process occurs slowly if the samples are carefully preserved but can occur rapidly when the samples are exposed to unfavourable conditions, such as warmth, moisture or sunlight. The degradation process can result in the loss of some STRs while others may still be detected. This problem can also occur if the samples are very small. 'Missing' STRs obviously cause problems with interpretation.[33]

DNA profiles can also contain 'spurious STRs' that result from technical artifacts. These artifacts arise during the process of producing a DNA profile in the laboratory and analysing it by computer; they are unavoidable. It is usually possible to distinguish them from real STRs, but this may not always be the case. There are no generally accepted criteria to discriminate between artifacts and genuine data, and so the experts are often forced to rely on their 'professional experience' to decide.[33]

Interpreting DNA profiles is particularly difficult when a sample contains a mixture of DNA from more than one person.[13] This is quite common in the case of scene of crime (SOC) samples. The high sensitivity of the tests makes it easier to detect DNA from everyone present at a crime scene, even if they leave only a minute trace. The strongest profile does not always come from the person who last held an object, but is dependent on the individual's genetic make-up.[20]Thus genetic profiles from an object handled by several people, for example a door handle, may be very difficult to unravel. It may even be difficult to be sure of the exact number of people contributing to a sample, particularly if they have similar STRs. It is difficult to 'sort' the STRs and the presence of one source of DNA can mask that of another.[24] There are no simple rules to help with interpreting 'mixtures'.

Making sense of DNA data is therefore very complex, and sometimes even the experts get it wrong. There have already been a number of cases where people have been wrongly convicted on this basis in the USA (see Box D). Since profiling is not a precise science, there is also a danger that the experts could be intentionally or unintentionally biased.[33] When faced with ambiguous results, an expert may be tempted to interpret the evidence in a way to help 'make the case'.

What measures are taken to reduce the risk of errors in interpreting DNA profiles?

Bias can be avoided by ensuring that DNA profiling is carried out by independent analysts who are not given information about the suspects or the crimes under investigation. Errors in analysing CJ samples are minimised by requiring a second sample from the accused to be analysed and used as evidence in court, rather than the sample that led to the original match. However, there are no simple ways to avoid errors in interpretation of SOC profiles, other than to have more than one expert analyse complex cases. It is therefore important to reinforce the message that DNA evidence is not as conclusive as is sometimes claimed, particularly when such evidence is considered in court (see Section 5.3).

Box D: Misinterpreting DNA profiles leads to wrongful convictions[24;26]

Case 1: In 1997, Timothy Durham of Tulsa, Oklahoma, was released from prison after serving four years for a rape that he could not have committed. At his trial, he was able to produce 11 alibi witnesses who placed him in another state at the time of the crime, but he was still convicted of raping an 11-year-old girl and sentenced to 3,000 years in prison. The prosecution's case rested on three pieces of evidence: he was identified by the victim; a hair found at the crime scene was shown to be similar to his; and a DNA test showed that his profile matched that of the semen recovered from the girl. A repeat DNA test later revealed that the initial result was a false positive that had arisen because of errors in interpreting a mixed sample. The lab had failed to completely separate the male and female DNA and the combination of STRs from the two sources produced a profile that could have included Durham's.

Case 2: Josiah Sutton was also victim to errors in DNA analysis and reporting, and spent nearly five years in prison for a rape he did not commit. Sutton's conviction rested almost entirely on a DNA test performed by the Houston Police Crime Laboratory. Reanalysis later showed that the forensic scientists had made a mistake in concluding that Sutton's DNA profile matched a semen sample taken from the back of a car where the rape had taken place. The value of the evidence had also been overstated when it was presented to the jury. It was suggested that Sutton's DNA profile matched only one in 700,000 black people, when in fact it matched more than one in eight. His profile was one of many that could have been included in the mixed samples in the case.

(d) Adventitious matches false matches by chance

False matches can occur when the wrong person is linked to a crime through their DNA profile because the profiles match by chance. These are not simply 'statistical anomalies', but happen all the time.[1] Most result from matches between twins or close relatives. But false matches between *unrelated* individuals can also occur (see Box E). The matching process also occasionally throws up more than one name, but this most often occurs because a person has submitted more than one sample using different identities.[34] The NDNAD's annual report states that to date no false matches between *full* profiles have occurred that cannot be explained by processing errors or individuals being related. However, it estimates that false matches could happen purely by chance one or two times over the next five years because of the increasing size of the database.[1]

The probability of a false match becomes greater if only partial DNA profiles are analysed. There is also a risk that DNA profiles of people from ethnic groups where strict marriage customs sometimes apply, such as Ashkenazi Jews or caste Hindus, will match far more frequently than the usual statistical calculations suggest.[35] It is claimed that careful police work will compensate for problems caused by false matches. However, this assumes that it is a simple matter to trace people's relatives and that it is possible to obtain more samples and fuller profiles.

BOX E: A false DNA match leads to wrongful arrest

In April 1999, Raymond Easton was visited by Swindon police and asked to give a blood sample to help with the investigation of a burglary over 200 km away.[35] Mr Easton was unconcerned because he knew that several family members would confirm that on the night in question he had been at home caring for his sick daughter. He was also suffering from advanced Parkinson's disease and could not drive, dress himself or walk more than 10 metres unaided. However, he was unaware that his DNA profile, obtained from a sample he had given four years earlier during a domestic dispute, had matched a DNA profile found at the scene of the crime. Mr Easton was subsequently arrested for the burglary, purely on the basis of the DNA evidence. He was taken to a police cell where he was kept for several hours before being granted bail. It finally came to light that Mr Easton had been a victim of 'an adventitious cold hit' a false match that occurred by chance – but it still took three months for the charges against him to be dropped. Changes to the DNA profiling process since this incident have reduced the chances of similar false matches[36] but this does not mean the chances have been reduced to zero.

What measures are taken to reduce the risk of false matches?

In order for DNA evidence to be admissible in court, the suspect has to provide another sample, usually another mouth swab. This new sample, called a case work (CW) sample, is processed independently and the new DNA profile compared directly with the original profile from the crime scene. This additional step helps to check for any 'false' matches that might have occurred due to errors in processing the original CJ sample taken on arrest. Case work samples can also be taken within a short space of time of a crime being committed from an individual arrested at or near a crime scene.[18] In these cases a match is sought directly between the arrested individual's DNA profile and the DNA evidence from the crime scene, without needing to search the NDNAD.

Only DNA profiles from CW samples can be used in court, profiles from CJ samples are for use during investigations only. However, scene of crime (SOC) samples, which may contain mixed, degraded or contaminated DNA, cannot be double-checked. Nor can taking a second sample identify the rare cases like Mr Easton's when a profile match may occur by chance, rather than because of processing errors. Proof of innocence or guilt is therefore crucially dependent on the strength of any corroborating evidence.

5.3 Using DNA evidence in court

There is no doubt that the use of DNA evidence has been an extremely effective means of securing convictions for many crimes, including a large number of property crimes and a much smaller number of rapes and murders (see Box F).[19]However, it is also clear that this type of evidence can be overly compelling and that the problems of false positives and negatives can sometimes get forgotten.[33] DNA evidence alone is not sufficient to secure a conviction.[14]

When the courts are presented with DNA evidence it is therefore essential that they:[37]

- are given a balanced view of the information, that takes account of the possibility of errors.[28;29] There is a standard way of presenting DNA evidence in court that is intended to ensure this;
- take a cautious view of the evidence,[10] recognising that it can show only that a suspect was present at the scene of crime but says nothing more about guilt or innocence;
- are convinced by additional independent evidence that links the suspect to the crime. This is why corroborating evidence, such as witness statements, is always required;
- consider where the DNA profile came from and how it could have got there. For example, even a DNA profile from a semen sample could result from consensual sex

rather than from an alleged rape. DNA found on a cigarette butt may have been planted at the crime scene or be there for reasons unconnected with the crime.

Box F: The use of the NDNAD in successful police operations[1]

These examples from the NDNAD annual report show how matches between DNA profiles can help the police with their investigations. The report does not give details of the corroborating evidence that would have been required in court.

Operation Phoenix: In January 2003, Mark Wilkinson from Roker, Sunderland, was found guilty and jailed for five years for the rape of a 19-year-old student back in 1996. He was asked to give a routine sample when arrested for urinating in a South Tyneside street. His DNA profile then linked him to the rape.

Operation Flame: £500,000 was stolen during 18 raids on post offices in north Wales, the north west and the Midlands. The raids all followed the same pattern. Post office staff were attacked in their homes, taken to their place of work and held hostage while they waited for safe time-locks to be released. DNA evidence proved crucial to finding the suspects. A full DNA profile was obtained from a balaclava found in a car used during the first raid. The same profile was obtained from the screws used to fix a false number plate onto another car used in three of the other robberies. This profile was found to match Alan Motion, whose information was on the NDNAD as a result of a minor domestic incident. Similarly, a DNA profile from the handle of a safe opened during a raid in Staffordshire was found to match that of John Barlow. Both men were convicted of conspiracy to commit armed robbery and sentenced to 16 years in jail.

Operation Vagabond: John Wood was arrested for stealing £10 of groceries from a supermarket but was subsequently found to be responsible for an unsolved sex attack on two young girls that had taken place three years earlier. A profile from the routine DNA sample taken in connection with the theft was found to match a profile from the crime scene held on the NDNAD. Wood's two victims, aged 9 and 11, had been subjected to an hour-long attack at their Canterbury home. Wood pleaded guilty to rape and indecent assault and was sentenced to 15 years in prison.

There are some concerns that the criminal justice system does not do enough to help jury members distinguish between powerful DNA evidence and weak, misleading data.[33] There are often case-specific issues and problems that greatly affect the quality and relevance of DNA results that must be brought out into the open. It is argued that defendants should be given resources to have independent experts take a second look at the DNA evidence, to indicate whether there might be problems and what their significance might be. Otherwise it is all too easy to accept lab reports at face value without assessing whether the actual test results fully support the experts' conclusions.[33] The use of DNA evidence in court is not foolproof. However, challenges to the use of DNA evidence in British courts have been rare.

6 What Laws Govern the Use of the NDNAD? What are the Limits on Police Powers?

Legislation determines how the police can use the NDNAD.[38] It sets the rules as to when a sample can be taken, whose profiles can be added to the NDNAD and when the data and the sample must be destroyed. England and Wales have some of the most permissive laws around the use of forensic DNA, making the NDNAD one of the most extensive databases in the world. The law in Scotland is different and, although DNA profiles from Scotland have been added to the NDNAD in the past, there is now a separate database. DNA profiles from Northern Ireland are not yet routinely added to the NDNAD.[36]

6.1 England and Wales: legislation relating to the NDNAD

The Criminal Justice and Public Order Act 1994 created the conditions under which the police can legitimately take, retain and use DNA samples. Although this led to the establishment of the NDNAD in 1995, the existence of the database was never formally established in any legislation. Since 1994 the UK Government has provided consistent financial and legislative support to greatly expand the use of DNA profiling for a widening range of offences. Britain has made some of the swiftest changes in law to make such extensive use of the NDNAD possible.[13] A brief history of the legislative changes in England and Wales is given in Box G.

On 4 April 2004, police powers were extended once again to allow DNA profiles, fingerprints and other information to be taken without consent from anyone simply arrested on suspicion of any recordable offence. This includes all but the most trivial offences. The new legislation also allows the police to keep this information indefinitely, even if the person arrested is *never charged.*[39] This gives the NDNAD the most extensive list of people in the world. No other police force has greater freedom to obtain, use and store genetic information from its citizens.[14]

Challenges to the legislative changes

These rapid and far-reaching changes in legislation have been made with very little public debate. The latest changes to the legislation, which came into effect in April 2004, were introduced via a late amendment to the Criminal Justice Bill, tabled less than a week before the Bill was debated in the House of Commons.

On other occasions, changes have been made on the back of high-profile cases, making it difficult for people to voice concerns without seeming to oppose the conviction of criminals. For example, there was public uproar in 2000 when a murderer escaped conviction on the basis that crucial DNA evidence had been obtained from an illegally held sample.[41] This furore was used to push through legislative changes in 2001 which allowed the police to keep all DNA profiles and samples indefinitely. It seems that a similar approach has been used to gather public support for such legislative changes in Australia (see Box H).

Box G: A brief legal history of the NDNAD[1;6;12;19;23;40]

1984 The police were allowed to ask doctors to obtain a blood sample to use for DNA testing to help with the investigation of serious crimes, with the consent of volunteers. However, forensic DNA technology was still fairly limited in its use at this time.

1993 The Royal Commission on Criminal Justice recommended that a forensic DNA database be established. The main driver was concern about public confidence in the criminal justice system as a whole, following a number of high-profile miscarriages of justice, for example the Birmingham Six, who had been jailed for planting an IRA bomb, but whose convictions were subsequently quashed. The database was proposed as a more objective form of forensic identification, with as much potential to eliminate suspects as to secure convictions.

1994 The Criminal Justice and Public Order Act (CJPOA) enabled the NDNAD to be established. The Act changed the rules around collecting tissue samples by reclassifying saliva samples and mouth swabs as non-intimate and changing the circumstances in which a non-intimate sample could be taken without consent. This meant the police could now take samples without assistance from a doctor and could collect mouth scrapes and hair roots by force if necessary. It also changed the rules around the type of offence, from any 'serious, arrestable' offence to any 'recordable' offence (these include all but the most trivial offences) which greatly widened the pool of suspects. The law also stated that if a person was subsequently found guilty, their information could be stored on the database and their sample kept indefinitely; if they were not charged or were acquitted, the data and the sample had to be destroyed.

1997 The Criminal Evidence (Amendment) Act allowed non-intimate samples to be taken without consent from individuals who were still in prison having been convicted for a sex, violence or burglary offence prior to the NDNAD being set up in 1995.

2001 An extension to the Police and Criminal Evidence Act 1984 (PACE) made amendments to allow all samples (and fingerprints) to be retained indefinitely, irrespective of whether the person had been acquitted. Another amendment also allowed samples to be retained indefinitely from volunteers taking part in mass screenings, on the condition that they had freely given their consent.

2004 An extension of the Criminal Justice Act came into effect on 4 April 2004. This latest development allows the police to take samples from anyone who has been arrested and taken to a police station in connection with any recordable offence, and to store the genetic data and samples indefinitely.

Box H: Promoting public support for changes to forensic DNA legislation

In early 2000, when forensic DNA legislation was approaching a vote in the parliament of New South Wales, the Australian police staged the country's first ever mass DNA testing.[41] Almost all of the adult men in the town of Wee Waa were asked to give samples to assist the investigation of a rape of a local pensioner. Those who criticised the draconian legislative package were portrayed as effectively being in favour of the rape of elderly women. The Bill passed without significant amendment. The tactic was repeated in more recent years when the murder of an English tourist and the abduction of his companion were used as the rationale for allowing unregulated exchange of police DNA information between the states in Australia. The practical consequences are that standards relating to police use of DNA data have been effectively reduced in every state to the lowest standard operating in any of them.

Two people have legally challenged the legislation that allows the permanent retention of DNA profiles and samples on the NDNAD in the case of 'S' and Marper v The Chief Constable of South Yorkshire, QBD Court, March 2002.[1] Mr Marper and 'S' (a 12-year-old boy who cannot be named) were both acquitted of all charges against them. They made two appeals claiming that the subsequent storage of their samples was an infringement of their right to privacy and contravened Articles 8 (part 1) and 14 of the European Convention on Human Rights.[42] Part 2 of Article 8 of the European Convention allows an infringement of an individual's right to privacy for 'the prevention of disorder or crime'. The legal question was whether the invasion of the privacy of 'S' and Mr Marper was 'proportionate'. The Lord Chief Justice's ruling was that this invasion was 'proportional to the benefits to the public'. This judgment has now been endorsed by the House of Lords.

6.2 How England and Wales compare to other countries

Comparisons with other European countries

In June 2001, the EU recommended that all member countries establish compatible forensic DNA databases, analysing the same set of STRs to produce their DNA profiles.[14] Therefore all European forensic laboratories are now using similar profiling technology. This allows data to be exchanged between countries to help with international criminal investigations. In 2002, Interpol (an international intelligence agency promoting collaboration among intelligence agencies around the world) conducted a DNA database inquiry which showed that 34 out of 46 European Interpol members already had or were planning to have a national forensic DNA database.[13;14;43]

The national laws governing the use of these databases vary a great deal, particularly in relation to whose profiles are added to the database and for how long the genetic information and samples are stored. The major differences, as they stood in October 2003, are summarised below. However, since the current trend is for legislation to change quickly and for databases to become increasingly inclusive, the range of samples that can be collected and stored may well have already increased.

Which offenders are added to forensic DNA databases?

Some countries include only DNA profiles from people convicted of specific types of crime or people expected to serve a particular length of sentence. Some require a court order, while for others data entry is automatic. For example in:

Sweden: profiles are added if the offender is expected to spend more than two years in prison.

Norway: profiles are added from people convicted of a serious crime, but this requires a court order.

Germany: profiles are added from people convicted of specific offences based on an evaluation of whether the person is likely to re-offend. A court order is also required.

Netherlands: profiles are added only if the DNA evidence has been crucial to the conviction.[19]

Who is added to forensic DNA databases?

In most countries, the profiles of individuals are added to the database only if the person is arrested for a severe crime or sexual assault. Only England and Wales, Austria and Slovenia include profiles from people arrested for any recordable offence.

When are DNA profiles removed from forensic DNA databases?

Most countries remove the DNA profiles of convicted offenders after a period of five to 20 years. Only England and Wales, Austria, Finland and Norway retain these profiles indefinitely.

In the case of suspects, most countries remove the profiles if the person is acquitted or charges are dropped. Only England and Wales retain this information permanently.

When are tissue samples destroyed?

A number of countries destroy the tissue samples once the DNA analysis has been completed, for example Belgium, Germany, the Netherlands and Norway. Other countries, including Austria, England and Wales, Denmark, Finland, Hungary, Slovenia and Switzerland, retain duplicate samples in storage.

Comparison with the USA

The forensic database in the USA, the Combined DNA Index System (CODIS), has been modelled on the NDNAD and connects all of the 50 different state databases to a national computer network.[19] Each state has developed its own forensic database laws while following certain federal guidelines.[43] While all states add the profiles of people convicted of violent crimes to their database, only some states have passed laws to allow suspect profiles to be added. However, there are plans to expand CODIS in two ways: first, to include DNA profiles from persons convicted of 'any felony' (a felony is a serious crime for which the punishment is prison for more than a year); and, second, to allow all state authorities to enter DNA profiles from people who have been 'indicted' (accused of a crime) or who have waived indictment for a crime, i.e. where charges have been dropped.[24] This would bring the US system directly in line with England and Wales.

6.3 Concerns about the legislation protecting our civil liberties

Originally, DNA profiling was used to attempt to match an individual suspect's DNA with a DNA sample from the scene of a crime. A database is not necessary for this case-by-case approach, since a sample can be taken from a known suspect once they are in police custody, or from a 'mass screen' of a small population thought to contain the suspect (for example all the people in a nearby village). However, it was recognised early on that establishing a database could reduce the chances of a perpetrator evading a mass screening.

Later, the idea developed that the NDNAD could capture information on the 'criminally active population' based on evidence that a large proportion of all crime is committed by a relatively small number of people. The policy of including a population of 'suspects' on the database, including people who have been arrested but not convicted, was first announced by the Prime Minister in 2000.[36] The NDNAD now permanently retains personal and genetic data from an increasing number of innocent people:[19] this includes people who are arrested but either not charged or later acquitted of a crime. It also includes a much smaller number of people who take part in mass screenings for elimination purposes and consent to have their profiles entered on the database, rather than having them destroyed (see Section 9.1). As a result of

the recent changes in the law the number of people on the NDNAD is set to expand from around 2 million to some 5 million people.[4] Many critics believe this expansion of the NDNAD poses a significant threat to our civil liberties.[44]

Are we citizens or suspects?

Putting large numbers of people on the NDNAD effectively creates a class of people who are permanently under suspicion even though they may never have been convicted of any wrong doing. Being on a permanent 'list of suspects' may subtly alter the way in which the state sees us and how we see our fellow citizens.[5;45] The NDNAD is also the only database that keeps a person's 'criminal' record indefinitely, no matter how trivial their offence. This creates the possibility that simply being on the list could be used to justify further restrictions in the future, such as refusing some types of employment or travel documents, or subjecting people to additional surveillance (see Box I). Ultimately, it could provide a powerful means to track some or all of the individuals on the database, using traces of their DNA. These concerns relate not so much to taking DNA samples during an investigation, but to the long-term implications of retaining personal and genetic information on the database indefinitely.

It is sometimes argued that 'only the guilty would have something to fear' from being added to the database.[5] But this ignores the history of the misuse of information about citizens by both communist and fascist regimes in Europe and the dangers of creating a 'surveillance society'.[46]

Misuse of the NDNAD could also reinforce discriminatory policing, since it could well result in a disproportionate number of people from black and ethnic minority (BME) groups being convicted and sent to prison.[13] There have already been serious miscarriages of justice in the UK that have led many members of BME groups to hold very negative perceptions of policing.[2] There are also serious concerns being raised by the new anti-terrorism measures that could impact disproportionately on some types of people, such as people of Middle Eastern appearance or people involved in political protest (see Box I).

Box I: New anti-terrorism measures and civil rights

Anti-terrorism laws, racial discrimination and political protest: In the USA, new anti-terrorist laws have been enacted which are likely to compound problems of racial discrimination.[47] The Terrorist Identification Database Act of 2003 allows DNA samples to be collected for the purpose of 'detecting, investigating, prosecuting, preventing or responding to terrorist activities'. There are huge penalties for those who refuse to give a sample – fines of up to $200,000 or imprisonment for a year. Critics are concerned this will lead to widespread testing of DNA from people of Middle Eastern appearance and could be used to detain political activists and suppress legitimate political protest. In England, the new anti-terrorism laws introduced in 2000 have already been used against peaceful anti-war protestors.[48]

Visa restrictions for people arrested but not convicted: Countries like Britain are part of the US Visa Waiver Programme, which makes travel to the USA much easier. New restrictions mean that people who have been arrested now have to apply for a visa, even if they have never been convicted. In addition, the Rehabilitation of Offenders Act (which sets a time period for each offence after which 'spent' convictions do not have to be revealed) does not apply in these circumstances. This means that some people who have been arrested but not convicted, as well as others who have a past 'spent' conviction, will now have to make an expensive US visa application and may have their travel via the USA prevented or delayed.[49] There are concerns that the permanent records on the NDNAD could be used to extend these restrictions in the future.

7 The Future of DNA Profiling

There is a lot of interest in research to improve and expand DNA profiling in the future.[1] This research has three main goals:

1. to automate procedures and thus reduce the possibilities for human error;
2. to reduce the time it takes to generate a DNA profile – since the quicker the police can get to their suspect, the more likely they are to find them with incriminating evidence, for example with the stolen goods still in their possession;
3. to use the genetic information in samples from SOCs to predict the characteristics of a suspect. This may be useful in cases where the only intelligence information is the DNA profile.

Private companies in particular are investing heavily in research in these areas which are discussed in more detail below. As well as opening up new opportunities, this research also raises new areas of concern.

7.1 Predicted changes to DNA profiling

Carrying out a different type of DNA analysis

Two companies in the USA, Applied Biosystems and Orchid Biosciences, have developed a DNA identification technique that does not rely on STRs but looks at different areas of the DNA called single nucleotide polymorphisms (SNPs, pronounced 'snips').[50] SNPs are minute differences in the DNA (a change at a single base in the DNA sequence) that occur naturally in the population. Every individual has a unique pattern of SNPs. The advantages of using SNPs as a means of DNA profiling are that: [12]

they can be detected in very small bits of DNA and are therefore useful to analyse degraded samples, particularly those from crime scenes (SOCs);

they are simpler to analyse and therefore make it easier to automate the process;

because they are found in genes (the parts of DNA that are thought to be most important in influencing biological differences in health or appearance) they may be able to provide more information about a suspect, for example predicting their physical characteristics.

However, it seems unlikely that SNP-based DNA profiling will replace STR analysis in the very near future, except perhaps in a few special cases. In particular, there does not appear to be any advantage to changing the DNA profiles kept in forensic databases to SNPs. Such a change would require all the millions of samples on databases worldwide to be reanalysed, which would be prohibitively expensive and simply impossible in many countries where samples are not retained.[14;51] In addition, only a few SNPs may be identifiable from degraded crime scene samples and these may not match those that might be used in a future SNP-based forensic database. STR profiling also has important advantages over SNPs:

It is better for analysing mixed samples because people vary a lot more in their STRs. In the case of SNPs, people tend to fall into one of two to three categories, so that it may be more difficult to dissect out individuals in any mixture.

It has greater predictive power. 50 to 100 SNPs would have to be examined to get the same results as looking at ten STRs. The technology is not yet able to generate this amount of information very quickly, although this could change in the longer term.

STR profiling relies on non-coding DNA and therefore poses less of a threat to our right to privacy. In contrast, the use of SNPs could allow the police access to much more

personal genetic information, including information about people's health. This could be avoided only if the analysis were carefully restricted to SNPs from non-coding regions of DNA.

For these reasons, most experts believe that for the foreseeable future SNP technology will be useful only for very specialist applications. For example, it is particularly useful for identifying victims of mass disasters where DNA samples are highly degraded; it was used very successfully to analyse samples from the World Trade Center.

Although it seems unlikely that forensic DNA profiling will change radically in the future, the possibility of such changes is often used to justify the retention of samples and continued investment in SNP-based research. The private companies now carrying out DNA profiling are particularly strong advocates of the SNP technology.[52] However, they may be being driven by the potential commercial gains rather than any real practical benefits. There is a danger that the FSS will be swept along in the tide of this new technology, in response to these commercial forces (see also Section 8.1).

Improving the technology

New handheld DNA testing kits are being developed which could be used as mobile DNA profiling laboratories. It is claimed they will be able to generate results at the scene of a crime in as little as 15 minutes.[53;54] While there have been reports of prototype kits being tested successfully, they have yet to be introduced into routine practice.

7.2 Using DNA profiles to predict the characteristics of suspects

The expectation is that the Human Genome Project will eventually identify the genes that influence physical characteristics such as skin and eye colour, height, weight and facial features. Some scientists believe that this information could generate a description of a suspect from the SOC sample alone.[17] Researchers are also looking at how to predict a person's health status or behavioural traits from their genetic make-up. The Custodian of the database, Dr Bob Bramley, has said that ideally the police want a description along the lines of 'a 6ft 3in man with red hair and a tendency to obesity'.[55] Some of these applications may be unachievable and others are a long way off, but some relatively rare genetic disorders can be predicted from a person's genes. There is considerable interest in this type of research, particularly around the following areas:[56]

Predicting ethnicity

Research in this area falls into two categories:

(1) trying to find specific DNA sequences that can predict ethnicity[57]

(2) looking at the frequency of the usual ten STRs to see whether these vary among different populations. If this proves to be the case, the FSS hopes that the DNA profiles already on the NDNAD could be used to predict where a suspect comes from.[58]

Both approaches face serious difficulties.

The first approach relies on there being a relatively simple relationship between a person's genes and their ethnic origins, so that testing for particular genes can be used to make reliable predictions. Many researchers believe that human 'races' overlap so broadly that it simply will not be possible to predict someone's ethnicity from their genes.[57] (The concept of ethnicity is different from race. Ethnic groups are groups of people that share characteristics that include geographical and ancestral origins, culture and languages. Racial groups share biology or genes.) At best it seems that genetic markers can indicate whether a person's ancestral

background lies in one of four distinct historical populations East Asian, European, Native American and African[40] and research is continuing in this area. But these markers say little about the person's more recent origins. Therefore, it seems that this approach is unlikely to lead to meaningful predictions.

The second approach is distinct in looking for statistical relationships between DNA profiles and ethnic appearance. The ethnic origins of known suspects on the NDNAD are based on the best guesses of the police, which in turn are based on the suspect's appearance.[58] These categories therefore have no biological meaning. Similarly, the DNA profiles on the database are based on 'non-coding' parts of DNA that are thought to have little to do with appearance or ancestral origins. The idea behind looking at the frequency of the usual ten STRs in different populations is that it does not matter that these links have nothing really to do with biology. Instead, it is hoped that these frequencies will be the same in different ethnic groups in the general population as they are on the database, and that they can therefore be used to predict the likelihood that a SOC sample comes from a person from a particular ethnic group. However, the assumptions that the people on the database are representative of the general population and that there is a fixed relationship between the frequency of STRs and ethnic appearance are both highly questionable.

As with all race-related research, these approaches have been criticised more generally because there is a danger that they could reinforce existing race discrimination and racial prejudice.[57] This is a concern worldwide (see Box J).

Box J: The potential for DNA profiling to reinforce racial prejudice[59]

Forensic scientists at the National Research Institute of Police Science in Tsukuba, Japan, are planning to set up a database that will allow police to predict a suspect's ethnic origin and physical appearance. The Japanese authorities cite the increase in crimes committed by 'foreigners' as justification for the project. The database will gather information that could be used to distinguish different populations including data on ethnicity; blood type; genes affecting people's metabolism, hair and skin colour; and different viral infections. It is thought to be the first database that will try to attach an ethnic profile to an individual's DNA. However, critics argue that this initiative serves only to scapegoat foreigners and ethnic minorities for Japan's social and economic problems. The number of foreigners convicted of murder – 41 in 2003 – is actually decreasing, while the number of thefts by foreigners, although increasing, amounted to only 280 convictions out of 4,151.

Predicting skin colour

Because skin colour is a simple physical characteristic, unlike ethnicity or race, some scientists think that predicting skin colour from a DNA sample will be easier than predicting ethnicity. However, very few physical features are inherited in a simple way. Skin colour is thought to depend on several major genes plus many other 'modifying' genes. The only gene that is currently known to play a major role in skin colour is the melanocortin-1 receptor or MCR1 gene, which is linked with sun-sensitive, fair skin and red hair (see below).[60]Although predictions of skin colour may improve with further research, there will always be limitations to the predictive value of this approach.

Predicting hair colour

Red hair is associated with a particular form of the MCR-1 gene that causes the hair to contain more red pigment.[61] Testing for this gene can identify about 84% of redheads.[56] But since hair colour is influenced by so many genes, there is not a simple relationship between this gene and the colour of a person's hair.[62] For example, the test cannot predict the exact shade of red, which may be anything from ginger to auburn; and the effects are also age-dependent. Some

people are red-haired as children, but then go blond or brown as adults. The information that can be obtained from a DNA sample alone is therefore fairly limited. Predicting any other hair colour than red is likely to be even more difficult because many other genes are thought to be involved.[60] Again, predictions may improve in future, but it is unclear whether they will ever be reliable enough to be useful in most criminal investigations.

Predicting surnames

Since boys inherit both their Y-chromosome and, in many societies, their surname, from their biological father,[63] in theory there should be links between genetic information and men's surnames. In the one study that has been carried out to date, the researcher investigated his own name, Sykes. He found a single gene sequence that could be detected in 44% of men with this surname, which wasn't found in men with other names. However, this study was based only on a small sample. More importantly it also revealed that just a small amount of infidelity a few generations back would result in half the Sykes today not having the specific section of DNA. It therefore seems unlikely that such genetic tests will have much predictive power.

Predicting the state of someone's health

Some genetic variations inevitably lead to ill-health as in the case of Huntington's disease or sickle cell anaemia.[7] Genetic tests can be performed today which could show whether or not a SOC sample belongs to a person who suffers from one of these relatively rare genetic conditions. However, it is not clear whether this information would be useful to the police. Knowing that a person has a genetic condition may not reveal exactly *when* a person will become ill or *how severe* their illness will be.[7] The suspect may not show any symptoms or visible clues of their disease. This kind of test would also represent a major invasion of a person's privacy.

Similarly, there are no known genetic tests that could predict a 'tendency to obesity'. Many different genes are thought to be involved and none of them has yet been shown to be important for the vast majority of overweight people. Lifestyle factors (what people eat and how much exercise they get) have a much bigger influence. It is extremely unlikely that genetic information will ever be very useful in predicting whether a suspect is obese.

Predicting behavioural traits

Numerous research studies have claimed to find genetic links to behavioural traits such as aggression, homosexuality, depression or an addictive personality. None of these studies has stood the test of time.[64] In fact the whole approach to behavioural genetics has come under severe criticism (see Section 8.3). Again it seems extremely unlikely that such genetic tests could ever prove useful in predicting the personality or behaviour of a suspect.

The limitations of predictive DNA profiling

All the predictive tests developed so far have serious limitations. This is because there is not a simple relationship between genetic make-up and a person's physical or behavioural characteristics. Even in the case of simple traits like hair and eye colour, many different genes are involved and the environment has a huge impact[60] – people tan in the sun and go grey as they get older, to say nothing about the many different ways they can change these characteristics artificially. It is therefore impossible to predict the way a suspect looks or behaves with 100% certainty, raising doubts about how useful these tests can be for police intelligence.

A major concern is that the police could misinterpret such DNA evidence as a *certainty*, whereas the tests can really indicate only a *probability*. It may be misguided to use predictive genetics to generate a description of a suspect (see Box K). This is unlikely to lead to wrongful

convictions, because further evidence, including a DNA profile match, would be needed in court. However, it could waste valuable police time by narrowing down searches in the wrong direction and perhaps implicating innocent people during the investigation. There is also a danger that this type of information is used selectively to reinforce existing prejudices: for example, about race or skin colour. It is important for the police to be seen to be using information wisely and accurately if they want to maintain public trust in DNA profiling.

More serious privacy implications would arise if the NDNAD were to be upgraded in future to include SNP profiles not just from SOC samples but from every individual on the database. Although many genetic predictions are poor or unreliable, a few genetic tests can reveal important information about a person's health. It is the possibility that this kind of personal genetic information could be revealed that causes people to be worried about DNA samples being stored indefinitely and linked to the NDNAD (see Section 8).

Box K: Using DNA to predict a suspect's origins[53;65]

In April 2004, police reported for the first time that they had used DNA profiling in Britain to predict a suspect's origins. This approach was used in a widely publicised hunt for a serial rapist, who had attacked 31 elderly women in the south east of England in the previous 12 years. The man's DNA was said to contain 'strands from America, Europe and sub-Saharan Africa', a combination claimed only to be found in the Caribbean. Based on this information, the police announced that they were looking for a suspect from the Caribbean and furthermore that over 200 police officers with Caribbean backgrounds were being asked to volunteer for DNA tests to help determine which island the suspect might have come from.

This declaration ran counter to the conclusions of DNA Print Genomics in Florida, the company that actually carried out the DNA analysis. Zach Gaskin, their technical director, was quoted as saying: 'That's not what our test indicated.' He explained that although broad ethnic ancestry can be determined from DNA, geneticists cannot say with any certainty that an individual comes from a specific country.[66]

8 The Future of the NDNAD

As well as developments in science and technology, many policy changes and decisions may affect the future of the NDNAD and its use for other purposes.

8.1 The changing role of commercial companies

When the NDNAD was first set up, only the FSS produced the DNA profiles. Two commercial companies now also do this work and more are expected to apply in future. The idea is that commercial competition will produce the best-value service for the taxpayer. However, increasing the number of companies also increases the number of people with access to the samples, increasing the threats to privacy. It may also generate commercial incentives to introduce new technologies such as SNP profiling, which may not offer any real advantage over STRs (see Section 7.1).

The Government announced plans to privatise the FSS in July 2003, converting the FSS from a trading fund, into a Government-owned plc. These privatisation plans have been heavily criticised by some forensic scientists.[67] One concern is that this may lead to cost-cutting and a more error-prone service, and so reduce the reliability of DNA evidence. Another is that the priorities of shareholders may differ from the needs of the criminal justice system.[68]

8.2 Links to other national databases

The NDNAD is only one of a number of DNA databases being developed in the UK. DNA samples will also be collected from half a million people in Britain to form the UK Biobank.[69] The aim of this medical research database is to investigate genes linked to common diseases, such as heart disease and cancer. There have also been discussions about typing everyone's DNA at birth and storing this information on the new NHS electronic health records.[13;70] In effect this would create a national genetic database that uses each person's NHS number as a personal identifier.[17] These databases are likely to contain SNP profiles rather than the STRs that are currently used in the police database. The SNPs will have been chosen for their possible relevance to health or medical research. It is possible that in future the police may wish to compare SNPs from a scene of crime sample with the SNP profiles on a health or research database, to try to find a match and hence identify a potential suspect. An important issue to be addressed is when the police should be allowed access to this information (see Section 9).

There are also plans to develop new national registers, including a database to support the introduction of ID cards (see Box L). Although it has not yet been planned, there is a possibility that all these databases could be linked up at some point in the future, perhaps by including NHS numbers and Arrest Summons Numbers on the National Identity Register. This would provide the state with unprecedented abilities to monitor the UK population.[10;46;71] It is not yet clear how future Government agencies will be prevented from exploiting their access to this information.[44]

Box L: Government plans to develop national identity registers

The Government has announced that it will be introducing a system of national identity cards (ID cards) in Britain, details of which were published in a draft Identity Cards Bill in 2004.[72] The Home Office believes that ID cards can help in the fight against terrorism, serious crime, illegal immigration and the abuse of public services. However, many other individuals and organisations have raised concerns about the implications of ID cards for privacy and other rights.[73]

The new ID cards are likely to include electronic eye and fingerprint scans, but there are currently no plans to include DNA profiles. However, most concerns relate to the information which might be held on the ID cards database (called the National Identity Register), who will have access to it, and how it might be linked to other databases.[74] The National Identity Register could in future include any information about numbers allocated to a person 'for identification purposes'. For example, the Arrest Summons Number might be used to provide a link to the Police National Computer and the NDNAD.

8.3 Using the NDNAD for other purposes

Exonerating innocent people

Although much is made of the fact that DNA profiling is as likely to free innocent people as it is to convict the guilty, there is very little evidence of the technology being used to exonerate people in the UK.[75] There have been only a few cases where DNA profiling has been carried out after the original prosecution. This did not result in anyone being released from prison until as late as 2003, when Michael Shirley was absolved of the crime of rape and murder.[75] Overall, it seems that the police focus almost entirely on securing criminal convictions.

Post-conviction DNA profiling has yet to become an integral part of the UK criminal justice system. There are no resources available to identify or support the people who might appeal on these grounds. Nor has any official guidance been published to promote the use of DNA profiling to people already serving long-term prison sentences. This is in complete contrast to the situation in the USA where the Innocence Project has been set up exclusively for this purpose. The Project has so far resulted in 141 post-conviction DNA exonerations, including the release of 13 prisoners from death row.[24] The UK needs to consider how it can replicate that kind of success over here.

Using the NDNAD for non-forensic purposes

The maintenance of genetic databases is very expensive, which may well encourage people to consider using the NDNAD for other purposes.[10] There is always the possibility of 'function creep' where over time the technology introduced for one narrowly defined purpose is extended in use to other areas.

In the USA, various state laws already allow this to happen.[24] For example, a Massachusetts law allows disclosure of DNA records for 'advancing other humanitarian purposes' and Alabama allows access to its DNA population statistics database 'to assist with medical research'. The concern is that increasing the number of users also increases the threat to privacy.

In the UK, the Government has recently proposed setting up an additional 'Missing Persons DNA Database'. The police would need separate authority to speculatively search these DNA profiles against the NDNAD. The result of any searches and the samples would be destroyed once a body or a missing person had been identified.[76]

Using the NDNAD for research into criminal behaviour

The data stored in the NDNAD in combination with access to the stored samples could offer a wealth of information for researchers interested in studying criminal behaviour. There have already been studies that have tried to find genes linked to violent or sexual crimes or to find ways to use genetic tests to predict which people are more likely to re-offend.[77] However, there are strong arguments against using the NDNAD for research of this kind including:

Lack of consent

Using the NDNAD for research would violate the right of research participants to opt out of potentially controversial studies. Because consent would not have been given for research purposes, using the data would represent a major breach of privacy that would be difficult to justify (see Section 9).

Reinforcing prejudice and discrimination

There is a danger that behavioural genetic studies could contribute to an overly simplistic view of criminal behaviour. People may be led to believe that criminal activity is inevitable and influenced more by an individual's genes than their environment. The results of this research might then be misused to reinforce existing social injustices and discrimination. However, even the experts agree that if there is a genetic influence on behaviour, it is only very minor.[78]

Flaws in the overall approach

All research into behavioural genetics relies on an approach that has been subject to severe criticism.[79] Most studies of this type seem to be good at producing correlations but rarely generate any robust or meaningful evidence (see Box M).

Box M: The limitations of studying genetic links to criminal behaviour

The limitations of behavioural genetics are best illustrated by the results of a Danish study of criminal behaviour.[80] The study looked at whether the crimes carried out by boys who had been adopted were in any way linked to a criminal history in their biological or adopted parents. The research did find a relationship between the crimes of adopted children and their biological parents, but only in the case of house break-ins. It is hard to imagine how such specific criminal behaviour could be influenced by a person's genes. The results in fact suggest that adoption itself is a greater predictor of criminal activity and that genes have very little impact.

This point is illustrated by the following hypothetical example. If research were carried out in the USA to find genetic links to criminal behaviour, the genes influencing skin colour would probably be found to be linked with crime. This is because the majority of prisoners in the USA are AfricanAmerican. But it would be wrong to conclude that the genes that produce skin pigment cause criminal behaviour or for researchers to claim they had found a criminal gene. The results would demonstrate only a correlation that on its own would be pretty meaningless.

So far the NDNAD has not been used for research related to behavioural genetics. Since 1995, five research proposals have been submitted to the NDNAD Board for consideration. Of these, two were approved, two were rejected and, as of March 2004, one was still pending a decision. The two successful projects related to identifying suspects via their ethnic or family backgrounds and both were conducted by the FSS.[81] Neither project sought the informed consent of participants.[81] It remains unclear whether or not the DNA samples linked to the database have been used in any research. However, the database itself has been used for at least one potentially controversial project: attempting to link DNA profiles with ethnicity.[58] In the absence of transparent oversight mechanisms, the FSS needs to do more to convince the public that the samples and data are being adequately protected (see Section 9).

9 Are our Human Rights and Civil Liberties being Adequately Protected?

This question is best answered by reviewing the legislation and regulations that relate to the following key issues:

Whose profiles should be added to the NDNAD?

When should samples be destroyed?

How should sensitive genetic information be protected?

Who decides how the NDNAD should be used?

These issues will now be considered in turn.

9.1 Whose profiles should be added to the NDNAD?

There is a wide range of views about whose data should be held on the NDNAD and for how long. The question is how to balance the need to prevent crime with the need to protect people's privacy and other rights and freedoms.

Some people argue that the NDNAD should be expanded to include the whole UK population, and others argue that the current law should to be made more restrictive. Different issues arise in relation to people who have been convicted of a crime; people who have been acquitted or whose charges have been dropped; and people who volunteer to help with investigations. These are discussed below.

People who have been convicted of a crime

Many commentators have concluded that the NDNAD should be restricted to being a criminal justice database by containing *only* the DNA profiles of people who have been convicted of a crime. It is generally agreed that people lose some of their right to privacy as soon as they have been found 'guilty'. It is also argued that innocent people should not have to pay any penalty to the state, no matter how small that penalty is.[13;27;38]

A database of those who have been convicted of a crime would also seem to be a relatively efficient means of detecting and preventing crime. There is good evidence that in Britain some 100,000 people are responsible for almost half of all crime.[82] Some types of crime also follow a pattern of behaviour, for example showing continuing or escalating violence (see Box N). A database that includes the people who are most likely to reoffend might help to deter these criminals and, if not, help to catch them if they do reoffend. This would require the NDNAD to reflect a better understanding of the crime patterns of offenders and their likelihood of reoffending.

Box N: Taking samples from people who might reoffend

A recent Metropolitan Police study of over 400 offences discovered that at least 70% of men who had physically assaulted their partners also had a previous criminal history. Of those who had sexually abused a partner, one in four had committed offences outside the home and one in eight was described as highly dangerous. It appears that some of these men can be identified as serial offenders, going from one abusive relationship to the next, becoming progressively more violent over time.[83] However, only 29% of these men had been added to the National DNA Database. The authors of the study concluded that the police need to get better at using this type of intelligence to investigate and prevent further crime.

However, there are problems with this approach. One problem is that defining the 'criminal population' is not a simple matter. About 1 million people commit a crime each year. Every year, around 20,000 people leave the pool of 100,000 persistent offenders, while another 20,000 enter it.[82] Inevitably, a 'criminal database' will include some people who are never going to offend again.

Keeping records permanently on the database, particularly in the case of juvenile offenders, can also be seen as a problem because it undermines the long-standing principle of rehabilitation.[5] It can endorse the cynical view that anyone who has a minor brush with the law is likely to continue with a 'life of crime'.[38] This policy is in stark contrast to the regulations surrounding the retention of criminal records on the Police National Computer (see Box O). Only records relating to serious sexual, violent or drug offences can be retained on the PNC for life. The NDNAD is therefore the only database that keeps a person's 'criminal' record indefinitely, no matter how trivial their offence.

Box O: The Police National Computer

The PNC consists of a number of linked databases holding extensive data on criminals, vehicles and property.[84] The criminal database (called PNC Phoenix) stores information about the person's name; date of birth; gender; offence; and associated conviction data.[85] It also records whether or not their DNA profile is on the NDNAD.[18] An ACPO Code of Practice describes when records should be deleted from the PNC in order to be compatible with the Data Protection Act.[86] For example, if someone is acquitted or their case is discontinued the record should be removed within 42 days, except in the case of some alleged sexual offences, when records may be retained for five years. Most convictions are kept on record for ten years, but records for serious sexual, violent or drugs offences can be retained for life. For people who have been acquitted of sexual offences, an authorising officer must consider the circumstances of the case and consider whether data retention is justifiable to protect vulnerable people and prevent and detect crime.

Use of the PNC is being reviewed as a result of the Bichard Inquiry, set up after the Soham murders. A new Code of Practice will be produced for the PNC, covering record creation, review, retention, deletion and information sharing.[87]

The final problem is deciding how serious a crime must be for the loss of rights to privacy to be an appropriate punishment. A survey of public opinion[6] found that the majority of people were in favour of taking DNA samples from persistent criminals responsible for serious or violent offences, but were opposed to using this technology for fraud and shoplifting. This is in contrast to current law that allows DNA samples to be taken and retained indefinitely for all recordable offences (the majority of offences the police investigate),[88] including public order offences.[89] Therefore, even if the database were to be restricted to samples and data from convicted criminals, there may be arguments for restricting this further to certain types of crime. A distinction might be made between obtaining DNA profiles during an investigation and subsequently keeping them on the database.

Any decision to limit the size of the database is to some extent arbitrary and potentially discriminatory. However, a good compromise may be to follow the approach adopted for the retention of records on the Police National Computer. This recognises that different types of offence vary in severity and adopts an approach which is proportionate to the type of crime. It allows information to be collected in connection with any recordable offence, but limits the length of time over which this data can be held.

People who have been acquitted or whose charges have been dropped

While it is clear that the police need the powers to collect DNA samples from suspects so that they can investigate a crime, it is less obvious why they need to keep people on the NDNAD

once they have been acquitted or charges have been dropped. In the past these people have been treated just like any other citizen. Now, keeping them on the NDNAD means they remain 'suspects' for any future crime. This raises the concern that a record of *arrest*, rather than of any criminal conviction, will be used to restrict people's rights and freedoms (see Section 6.3).

The group of people treated as 'suspects' has also been broadened. Until recently a suspect was usually someone who had been arrested and *charged* with a recordable offence. DNA samples could be taken only from people in police detention who had *not* been charged in certain circumstances if:[18]

- they gave their consent in writing; or
- an Inspector authorised a sample to be taken because there were reasonable grounds to believe the suspect had been involved in a recordable offence, and the sample would assist in proving or disproving the suspect's involvement.

Now the police can take a DNA sample *without consent* from anyone in police detention who has simply been arrested for a recordable offence, even if they are not charged. This gives police the power to take and retain DNA samples in what may be an arbitrary and potentially discriminatory way. There is no need for the DNA sample to be relevant to the particular offence under consideration. Less evidence and oversight is also needed to arrest a person than to charge them. This could lead to:

- a disproportionate number of people from ethnic minority groups being included on the NDNAD as a result of discriminatory policing;[6]
- an abuse of police powers to collect surveillance information on peaceful protestors (see Box P);
- people being arrested simply to get hold of a tissue sample to make a speculative search of the NDNAD.[6]

Box P: Taking DNA samples from peaceful protesters

A famous example of environmental protest, opposition to the construction of the Newbury bypass, led to hundreds of arrests. By the end of the evictions of the protestors (2 April 1996), there had been 748 arrests, including 321 for obstructing the Sheriff and 306 for aggravated trespass.[90] Many of those arrested later had their charges dropped. There have also been cases where journalists have been wrongly arrested for trespass while photographing a protest.[91] Most of these people would now have their records permanently entered on the NDNAD – including those arrested but not charged – begging the question as to whether this is a justifiable loss of their privacy and raising concerns about future police surveillance.

Many people who are arrested are arrested for relatively minor public order offences, and nearly half have the charges against them dropped (see Box Q). This means that the NDNAD will now contain more and more samples from 'innocent' people where the subsequent loss of privacy may not be easily justified.

Box Q: What happens to people after police arrest?

Ten years ago a survey was conducted to find out what happened to the 1.75 million people who were arrested in 1993/4 (for both recordable and non-recordable offences).[92] The survey found that:

- Well over a third of suspects were detained for relatively minor public order offences: only 4% had been arrested for the most serious violent crimes (including rape).
- 85% were male and 15% were under 17.
- 78% were white, 13% black and 7% Asian: black people were more likely to be arrested than would be expected by their representation in local populations.
- 2% were considered mentally disordered and a third of these were detained solely for their own safety.
- Just over 60% had previous convictions.
- 87% were arrested on suspicion of committing an offence: the rest were held on warrant, as a place of safety or in transition between prison and court.
- 52% of suspects were charged; 20% had no further action taken; 17% were cautioned; and the rest were dealt with in various other ways.
- Of those arrested, 40% were eventually convicted, although the proportion was much lower for domestic violence cases (21%).

In contrast to the NDNAD, data retention on the Police National Computer draws a line between people who are convicted and those who are acquitted, with some limited exceptions, mainly relating to some people who have been acquitted of sexual offences in specific circumstances. This means data retention is restricted to a much smaller group of acquitted people, over specific lengths of time. Although these rules might change as a result of the Bichard Inquiry (see Box O) they will continue to be based on the idea that retention of data on acquitted people is justifiable only in certain specific circumstances. If similar rules were applied to the NDNAD, this would help to address concerns about the dangers of excessive state surveillance of the population.

People who volunteer to help with an investigation

People may volunteer to help with a police investigation if their sample is needed to interpret the evidence from a crime scene, for example to eliminate the DNA profile of the partner of a woman who has been raped; or to help narrow down the list of suspects in the case of a mass screening. These are the only people who are asked to give their consent. They are asked to give two types of consent. The first is their consent to their sample being used for comparison with an SOC sample. The second is their *non-revocable* consent to the police retaining their information and samples indefinitely. If this latter consent is not given, by law both the sample and the DNA data have to be destroyed.

It is debatable as to whether people can truly give their consent freely in these circumstances because refusal to give a sample immediately places a person under suspicion.[38] The police might also use unreasonable coercion to force people to take part (see Box R). However, the main concern is about the second type of consent, because it cannot be revoked. There are some doubts about whether people are provided with sufficient information about the two types of consent to be absolutely certain about what they are agreeing to.[88]

Recently, the Home Office introduced guidelines which provide a standard procedure for obtaining consent, using two different forms.[36] The new guidelines go some way towards addressing concerns about how consent is obtained from volunteers. However, it is important to remember that some information on the NDNAD is there only because people volunteered to give their samples for elimination purposes. The difference between volunteers' records and

the other records on the NDNAD is that they have no Arrest Summons Number and are not linked with corresponding records on the Police National Computer.

Box R: Freedom to give consent to providing a DNA sample

In England: The Metropolitan Police came under severe criticism after suggesting to black men in south London that their failure to submit to voluntary DNA tests was hampering an investigation into catching a serial rapist.[93] In a letter sent out to the local population, a senior detective wrote: '*Consider that the suspect is likely to refuse to provide a voluntary sample; catching him will be far easier if he is the only one.*' The detective also seemed to threaten people who refused to take part by saying: '*I will be reviewing the circumstances around your refusal and will notify you of my decision*.' This kind of intimidation makes a mockery of the principle of obtaining voluntary consent and will only serve to discourage local co-operation and support. Such an approach cannot be justified even in the most serious of cases.

In the USA: In Louisiana, there was a mass screening of hundreds of local white men to help with a case of rape and murder. Where people refused to give samples, police officers leaked their identities to the local press and employers, which in one case led to an innocent man being suspended from work.[10]

Expanding the NDNAD to include the whole population

There is some interest in creating a database with information on everyone in the UK. Some police officers and forensic scientists have argued that such a database would greatly increase their ability to solve more crimes more rapidly.[44] Treating everyone the same way is argued to be the fairest means of avoiding discrimination.[13] However, there are also strong arguments against expanding the NDNAD:[10;13;25;94]

- It would effectively infringe everybody's rights, including their privacy.
- It may be prohibitively expensive.
- A larger database may be slower to generate matches and more prone to errors, increasing the risk of wrongful arrest.
- A larger database could still be used in a discriminatory way (for example, by searching for everyone of a particular ethnic origin or everyone with a record of arrest).

Treating everyone as a suspect violates our rights to be protected from 'unreasonable searches and seizures'. It has been likened to forcing everyone to have their bags searched on leaving every shop[95] – a level of surveillance that some people consider excessive.

There are other concerns related to the ever-increasing expansion of the NDNAD. In particular, it seems to promote a criminal justice system that relies more on 'cold hits' than on thorough police investigations. This creates a more error-prone system which threatens the right to a fair trial and may result in people being wrongly accused or convicted.[15]

9.2 When should samples be destroyed?

CJ samples

The retention of CJ samples poses a bigger threat to privacy than the storage of data on the NDNAD, because these samples could provide unlimited amounts of genetic information about known individuals. In the case of samples from convicted criminals, overriding the individual's right to privacy may sometimes be justified in terms of the wider interests of society. However, even in these cases the usefulness of retaining samples after a DNA profile has been obtained is questionable. When a person is found to be innocent, there does not seem to be any compelling reason why their rights should be denied. England and Wales are alone in retaining samples from people who have not been convicted of any offence.

The importance of protecting human rights in the collection and use of samples and genetic information has been recognised by UNESCO in its 'International Declaration on Human Genetic Data'.[11] Article 21 specifically relates to the retention of forensic DNA samples. In an early draft of the declaration, this Article stated that '*samples should be destroyed if the person investigated is either not charged with an offence or is found not guilty of the offence*'. However, as a result of lobbying from the UK Government, the final draft was rewritten with the additional clause '*unless other wise provided by domestic law*'. The UK has therefore ensured that it can overrule the measures of protection provided by this internationally agreed code of practice.[96]

Can sample retention really be justified?

DNA samples remain the property of the police force which collected them, but are stored by the laboratory which analysed them (either the FSS, or one of the other suppliers) for an annual fee.[36]The FSS justifies the retention of CJ samples on the basis that they could be used to:[97]

upgrade DNA profiles if the technology advances;

investigate any possible errors;

provide additional evidence when it is not possible to obtain another sample from the suspect.

However, as outlined in Section 7.1, the likelihood of any future changes to DNA profiling is now quite small. In addition, both the investigation of errors and the confirmation of test results should necessitate obtaining and analysing a *fresh* sample, rather than returning to samples in storage. Although this might prove impossible in a few isolated cases, this doesn't seem to justify the wide-scale threat to privacy. Destroying CJ samples after DNA profiling would go a long way to removing many concerns.[13]

SOC samples

SOC samples are now retained indefinitely since DNA technology can help to resolve cases long after any crime has been committed. However, after a certain period of time has passed (the prescriptive period), the law states that a crime can no longer be punished, even if the perpetrator is found. This period is variable, but longer for more serious crimes. It has been proposed that prescriptive periods are extended to exploit the full potential of DNA profiling. However, there may be good reasons for keeping the current time limits. After longer periods of time, alternative explanations for a 'match' may be impossible to uncover: errors that may have occurred during sample collection/analysis might be impossible to detect; while a crucial witness who may have been able to confirm an innocent explanation for the presence of a person's DNA might be dead or missing. On this basis the most logical policy to adopt would be to destroy SOC samples as soon as the relevant prescriptive period has passed.

9.3 How should sensitive genetic information be protected

What sensitive information is stored on the NDNAD?

As discussed in Sections 3.3 and 4.1, by far the biggest threat to privacy is posed by the storage of samples used to obtain DNA profiles. The string of numbers in a DNA profile *on its own* probably contains no more information about a person than, for example, the number on their driving licence.[15] Although some researchers have suggested that one of the STRs may be linked to schizophrenia, the STRs themselves are not thought to contain any information about an individual's risk of disease.[6] As long as DNA profiling continues to analyse areas of DNA where there aren't any genes, it is unlikely to reveal much sensitive information. This reduces the threats to privacy and provides another argument against the introduction of profiling using SNPs (see Section 7.1).[27]

A comparison of DNA profiles, on the other hand, could reveal much more information by showing whether particular individuals are related. The use of 'familial searching' is a particularly sensitive issue, and therefore needs very careful handling. Such a major invasion of family life needs to be justified by the seriousness of the investigation (see Section 9.4).

Are there adequate safeguards to protect the data on the NDNAD?

The NDNAD is registered under the Data Protection Act (DPA) 1998 and operates in compliance with the Act and Government IT security guidelines. Access is restricted to staff employed by the database Custodian and is password-controlled with passwords changing regularly.[12;21] By law, the data can only be used for law enforcement, so access by other Government agencies for other purposes would be denied[1]. However the protection offered by these laws may not be sufficient to prevent the misuse of genetic information for the following reasons:

The DPA does not provide sufficient guidance as to whether any particular processing of genetic information is acceptable.[7] The 'fair' processing of genetic data may be assured only through the introduction of specific legislation.

The law would not prevent use of data from the NDNAD for crime-related research (see Section 8.3) that was carried out by commercial companies or Government researchers.

If the data were to fall into the wrong hands, there is no UK law that specifically prohibits genetic discrimination. In contrast, the European Convention on Human Rights and Biomedicine (1997) prohibits *'any form of discrimination against a person on the grounds of his or her genetic heritage'*. The UK is among 13 out of 43 countries that have not yet signed the Convention.

There is also always the possibility that existing laws will be ignored and in fact this has already happened. When the database was first set up in 1995, by law tissue samples and DNA profiles were supposed to be destroyed if suspects were proven to be innocent. It is now estimated that as many as 80,000 samples were held illegally until new laws were pushed through to allow samples to be retained indefinitely (see Section 6.1).[15]

There are also fears that the police will abuse their access to samples and data or allow other statutory organisations to do the same. This is not an abstract fear but one based on people's previous experience.[10] Police in the UK have already used a blood sample obtained for DNA profiling to carry out medical tests *without the suspect knowing* (see Box S). There are also a number of historical examples where the state has abused its access to medical or genetic data, including forced sterilisations, screening tests prohibiting marriage and privacy issues related to HIV screening. Therefore, concerns about state access to the NDNAD are clearly legitimate. Even the police are concerned about the potential for misuse of genetic information (see Box T) and many are reluctant to provide DNA samples for forensic databases.

Box S: Misuse of a sample taken for DNA profiling

In March 2004, it was reported that a man (whose identity is being kept confidential) discovered he had HIV while standing in the witness box.[98] A sample of his blood had been tested for the virus without his knowledge or consent. He became aware of this fact only while being questioned about his HIV status by a defence lawyer in court. Later it emerged that he had previously given a sample to the police for DNA testing in September 2003, when he had been arrested and then released without any further charges. The judge presiding over the case called for an inquiry and recommended that the man be offered immediate counselling.

Box T: Police refuse to give samples to forensic databases

In England and Wales:[99] Every police force has asked all officers who come into contact with scene of crime evidence to provide a DNA sample so that they can be eliminated from subsequent investigations. This information is kept on a database that is separate to the NDNAD and speculative searching is not allowed, so the police are not treated as criminal suspects. However, thousands of existing police officers have refused, based on the concern that their genetic information could still be used against them, for example in paternity suits. By 28 February 2003, the FSS had samples from about 48% of officers,[100] but this percentage will have increased by now as new recruits must now give a DNA sample as a condition of service. The Human Genetics Commission has criticised this regulation, arguing that it amounts to a requirement for a genetic test as a condition of employment.[88]

In Tasmania: In 2002, the Police Association of Tasmania told its members not to volunteer their DNA samples for elimination purposes.[101] The Association took the view that requests to provide DNA were an employment issue as well as a breach of its members' civil and human rights. It did not believe the proposed safeguards would adequately protect its members from misuse of their genetic information in the future.

Police access to other genetic data

Another important question is how much access the police are being given to the genetic data that already exists in people's medical records or from genetic research. Information about a person's genetic risk of ill-health could potentially be used to identify suspects, for example 'we are looking for a man with cystic fibrosis'. Currently the police are allowed to ask for personal genetic data from an individual's medical record, but only if they can prove that without this evidence 'the task of preventing, detecting or prosecuting a serious crime would be seriously prejudiced or delayed'.[102] The information they are given is limited to what is strictly necessary for a specific investigation, and they must guarantee that they will not pass on the information or use it for any other purposes. However, there are concerns about the lack of clarity around how specific a police request for information must be and the lack of oversight mechanisms to check compliance with the criteria.

It seems that the same principles will apply to requests for information from future genetic databases like UK Biobank (see Section 8.2). The UK Biobank Ethics and Governance Framework states that '*Access to the resource by the police or other law enforcement agencies will be acceded to only under court order*'.[69] However, again it is unclear under what conditions such a court order might be made available.

Concerns about police access to genetic information and the threats to our right to privacy will increase as DNA research databases expand.[103] There is a danger that a future NHS genetic database could, in effect, become a national forensic database without proper scrutiny or informed debate on its acceptable use.

9.4 Who decides how the NDNAD should be used?

Some of the ethical considerations around the use of the NDNAD do not seem to be adequately addressed by the current oversight mechanisms. These include:

Carrying out familial searches

Familial searches can be justified in some circumstances, for example if they provide the only means of tracking down a violent criminal (see Section 5.1). However, they risk revealing very personal information, such as non-paternity, to people who may be unaware of the truth. It is therefore essential that the seriousness of the crime can justify the invasion of family privacy.[44] As yet there are no published guidelines as to when such an approach can be considered

ethical and what the implications might be for data protection. This situation is clearly inadequate and open to abuse.

Using the NDNAD for research

Researchers using the NDNAD do not have to seek consent from participants or the approval of independent ethics committee to carry out their research. They have only to seek permission from the NDNAD Board (see below). Some of the research could be highly controversial, for example research on ethnicity and race (see Section 7.2) or research on 'genes for criminality' (see Section 8.3).

Getting independent ethical approval is an important safeguard to ensure that research is morally and socially acceptable. Seeking informed consent protects the freedoms, rights and dignity of the people who take part. Current procedures remove people's right to opt out of potentially controversial studies. Even people in prison are asked to give their consent before taking part in any scientific study. Consent should have to be obtained from the individuals on the database before genetic research is allowed to go ahead.

The National DNA Database Board

All decisions relating to the use of the NDNAD are taken by the National DNA Database Board, which also has responsibility for overseeing the effectiveness and efficiency of its operation.[1] The Board is chaired by the lead person on forensic science from the Association of Chief Police Officers (ACPO) and includes the Custodian of the database as well as representatives from the Home Office, the FSS, the National Crime and Operations Faculty, different police regions, and one representative from the Human Genetics Commission.

However, there are serious weaknesses in the governance and oversight structures currently in place including:

- the lack of transparency around how decisions are made and whether these decisions are really being made in the public interest;
- the lack of an independent oversight body to scrutinise uses of the database and provide guidance as to when familial searches are appropriate;
- the potential for major conflicts of interest because of the triple role of the FSS it is the main supplier of DNA profiles; it carries out out forensic research; and, as custodian of the database, it makes decisions about how the NDNAD should be used.[13]

As originally suggested by the Royal Commission in 1993, and since then by the House of Lords in 2001 and the Human Genetics Commission in 2002,[6] the oversight mechanisms could be much improved by creating a new, independent advisory body that includes lay members. This body would need to oversee the entire operation of the NDNAD from sample collection through to the production and use of DNA profiles as well as deciding what uses of the database were appropriate. Such an independent body would provide the public with much more reassurance that the data and samples were being properly used and protected.[17]

10 Conclusions

DNA profiling plays an important role in tackling crime. The police rightly have the powers to collect DNA samples during criminal investigations and use this evidence in court. However, there are important questions about the extent to which DNA samples and profiles should be kept indefinitely as part of the NDNAD.

At GeneWatch UK, we believe that the current operation of the NDNAD does not strike an appropriate balance between the rights of the individual and the interests of the public. While there is no doubt that society does have an interest in the detection and prevention of crime, this cannot be used to justify every infringement of the individual's right to privacy and the loss of our civil liberties. This is especially true for people who are not found guilty of any crime. In this regard we believe England and Wales needs to bring its criminal justice legislation more in line with the rest of Europe.

Questionable practices

We believe that the following existing practices raise serious concerns:

- retaining people's records permanently on the NDNAD regardless of the nature of their offence;
- including people permanently on the NDNAD who have been arrested but not charged, or who have been acquitted;
- retaining DNA samples, rather than just the DNA profiles and personal data;
- using the database for genetic research without consent.

Concerns for the future

There are reasons to believe that new technologies and new policies could rapidly expand the threats to privacy posed by the NDNAD and other DNA databases. These include:

- the potential expansion of 'familial searching' (looking for the relatives of a suspect) to a broader range of offences;
- the potential expansion of the NDNAD to include other genetic information (for example SNPs) which may be health-related;
- attempts to use genetic information to try to predict race, health status or behaviour;
- increasing expansion of the NDNAD, perhaps to the whole population;
- increasing 'back door' forensic use of DNA databases established for health or research purposes;
- the possibility that multiple Government databases will be linked via the proposed National Identity Register.

The need for public debate

Like others, we are concerned that the legislative changes to date have been introduced too rapidly in the absence of any meaningful public debate. We believe that further deliberation is needed to find out what the public think is a reasonable balance between protecting the right to privacy and protecting citizens from crime. The questions that need to be addressed include:

- When should samples be destroyed?

- Whose profiles need to be on the database to ensure the most efficient prevention and detection of crime?
- Does the NDNAD reinforce existing inequalities in the criminal justice system?
- Is expanding the NDNAD the most cost-effective way of detecting and preventing crime when compared to other measures, for example increasing the number of police officers?
- When should convicted criminals be allowed to reopen their case to seek exoneration via DNA profiling?
- Which databases should be linked together via the proposed National Identity Register?
- When should the police be allowed to access other DNA databases, set up for health or research purposes?

The Human Genetics Commission (HGC) is responsible for advising ministers on all developments in human genetics including their social, ethical, legal and economic implications. It has a clear remit to involve and consult the public and other stakeholders and encourage debate. Future changes to the rules of operation of the NDNAD should not be made by ministers without first seeking its advice.

Recommendations

GeneWatch UK believes that there are changes that could be made to the operation of the NDNAD which would protect people's rights and increase public confidence without compromising its role in fighting crime.

Recommendation 1: DNA samples (except samples from the scene of a crime) should not be retained once an investigation is complete. Only DNA profiles and personal data need to be on the database to find a 'match' for a criminal investigation. Research uses of the database itself (profiles and personal data) should be restricted to producing 'quality control' statistics on the type of data that has been added and how the data is being used.

This recommendation removes concerns that samples could be used for purposes other than identification, such as research into criminal behaviour, without the individual's consent. Suspects' samples need to be retained for a certain length of time so they can be analysed and the profiles can be checked. However, destroying the sample once an investigation is complete does not in any way restrict future searches for matches. All the information that is needed is stored in the DNA profile held on a computer. Physical samples do not need to be retained to prevent errors because a fresh sample must be taken anyway before DNA evidence can be used in court. Although it can be argued that samples may need to be reanalysed if the technology is updated, in reality upgrading the DNA profiling system used on the database seems to be both costly and unnecessary.

The right to consent or refuse to take part in research is an important right for individuals and for society. It is not necessary to use samples or profiles taken without consent to do legitimate genetic research. It is also questionable whether the NDNAD provides a robust source of data. Categories within the database such as 'ethnic appearance' are meaningless for scientific purposes and the DNA profiles and samples will not be representative of either the general or the 'criminal' population. Genetic research using the database is therefore likely to be misleading as well as controversial.

Recommendation 2: An independent body should be set up to review all future applications to access the data and samples for forensic and non-forensic purposes; to ensure standards are maintained; and to ensure public accountability and transparency.

We are concerned both about the current use of the NDNAD and the potential for the increased threats to privacy in the future. We think it is essential that the NDNAD is made more accountable to the public. We therefore believe that a new independent body should be created that includes lay representation. This body should be made responsible for deciding when 'familial searching' is allowed, rather than leaving this decision to the police alone.

This body should also review the merits of methods which attempt to predict the characteristics of individuals from DNA samples left at the scene of a crime. There is a danger that attempts to predict physical appearance, or other characteristics, may hinder rather than help investigations by providing producing misleading information.

Recommendation 3: An 'Innocence Project' should be established to investigate possible miscarriages of justice using DNA.

DNA profiling can be a powerful tool to help establish innocence as well as guilt. DNA evidence can also be misinterpreted and lead to miscarriages of justice. A project like the US 'Innocence Project' could help increase public confidence that DNA profiling is being used wisely to improve the criminal justice system in England and Wales. The current system does not assist in reviews of cases where there is reason to suppose people have been wrongly convicted.

Recommendation 4: An independent review of whose DNA data should be sampled and retained is urgently needed. Research on the use of the NDNAD, its effectiveness and the justification for including innocent people, should be conducted to inform the debate.

Like others, we are concerned that the legislative changes to date have been introduced too rapidly and in the absence of any meaningful public debate. We believe that further deliberation is needed to find out what the public would accept as a reasonable balance between protecting the right to privacy and protecting citizens from crime. The public should have a say as to whose data is included on the database and for how long.

There is no data available to evaluate whether crime detection will be improved by including DNA profiles from people who are arrested and not charged, or by continuing to hold data on people whose charges are later dropped or who are found to be innocent. GeneWatch UK's current view is that:

- **The personal data and DNA profiles from people whose charges have been dropped, or who have been acquitted, should be removed from the NDNAD (unless they were connected with a serious violent or sexual offence).** During the investigation stage, it will have been possible to check whether their profiles match those from any crime scene on the database. Keeping innocent people on the database effectively means treating them as criminals. This undermines the principle of 'innocent until proven guilty' and is open to abuse, particularly in relation to 'political' offences involving peaceful protest. Making this change would also bring the NDNAD more in line with record-keeping on the Police National Computer.

- **DNA samples should not be taken until a person has been charged**, **unless needed to help prove or disprove a suspect's involvement in a *specific* offence**. The process of charging someone with an offence is more formal than simply making an arrest. Waiting until a person has been charged reduces the risk that speculative searching for matches using the database is arbitrary and unfair or that someone could be 'framed'. This is an important safeguard to prevent the database being used in a discriminatory way.

- **The database should not be expanded to include the whole population**. Threats to privacy and civil rights are more likely to be increased than reduced by proposals to expand the database; it would not prevent the database from being used in a discriminatory way and would only serve to increase the potential for state surveillance. In addition, in the case of a larger database, the probability of false matches and the resources needed to investigate each match could increase disproportionately to the number of solved crimes.

- **People's personal data and DNA profiles should not be kept indefinitely on the database (except when they have committed serious violent or sexual crimes)**. Keeping records indefinitely raises concerns about civil liberties, particularly when offences are related to peaceful protest or political dissent. This practice also undermines the principle of rehabilitation. Records on the Police National Computer are removed after a certain length of time, depending on the seriousness of the offence. Records for serious, violent and sexual offences are kept indefinitely, but most other records are eventually removed. A similar system of restrictions on retention should apply to the NDNAD.

11 References

1. The National DNA Database Board. The National DNA Database Annual Report 2002-03 (2003) London: Forensic Sciences Services.
2. Wiliamson R and Duncan R. DNA testing for all. *Nature* (2002) **418**:585-6.
3. Factsheet: The National DNA Database (2004) London: Forensic Sciences Services.
4. Jobling MA and Gill P. Encoded evidence: DNA in forensic analysis. *Nature Reviews Genetics* (2004) **5**:739-51.
5. Kimmelman J. The promise and perils of criminal DNA databanking. *Nature Biotechnology* (2000) **18**:695-6.
6. Human Genetics Commission. Forensic uses of personal genetic information. Inside Information: Balancing interests in the use of personal genetic data. pp 145-60 (2002) London: Department of Health.
7. Staley, K. Giving your genes to Biobank UK: Questions to ask. (2001) Buxton UK: GeneWatch UK.
8. Privacy International, London (2003).
   www.privacyinternational.org/survey/phr2003/overview.htm
9. The General Assembly of the United Nations. The universal declaration of human rights (1948) The United Nations.
   www.un.org/Overview/rights.html
10. Irish Council for Civil Liberties. Human rights compatibility of the establishment of a DNA database: ICCL Position Paper (2003) Dublin.
11. UNESCO. International Declaration on Human Genetic Data (2003) UNESCO.
    http://portal.unesco.org/en/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html
12. House of Lords Select Committee on Science and Technology. Human genetic databases: Challenges and opportunities (2001) Examination of witnesses Dr Bob Bramley and Dr David Werrett, FSS and Dr Jill Tan, Home Office. pp 30-41. London: The Stationery Office.
13. Reilly P. Legal and public policy issues in DNA forensics. *Nature Reviews: Genetics* (2001) **2**:313-17.
14. Martin PD, Schmitter H, Schneider PM. A brief history of the formation of DNA databases in forensic science within Europe. *Forensic Science International* (2001) **119**:225-31.
15. Concar D. The DNA police. *New Scientist* pp 10-12. 5-5-2001.
16. The Forensic Science Service. Mouth swab to database: A guide to the DNA profiling process (2003) London: The Forensic Science Service.
17. House of Lords Select Committee on Science and Technology. Human genetic databases: Challenges and opportunities (2001) London: The Stationery Office.
18. Association of Chief Police Officers. DNA Good Practice Guide. Version 1 (2003).
    www.forensic.gov.uk/forensic_t/inside/news/docs/DNA_Good.pdf
19. Linacre A. The UK National DNA Database. *The Lancet* (2003) **361**:1841-2.
20. van Oorschot RA and Jones MK. DNA fingerprints from fingerprints. *Nature* (1997) **387**:767.
21. Bramley B. The National DNA Database: control and access (2002). London: Genetics and Law Conference.
22. Falloon M. DNA traps brick thrower who killed lorry driver. The Guardian. 20-4-2004.
23. Werrett DJ. The national DNA database. *Forensic Science International* (1997) **88**:33-42.
24. Simoncelli T. Retreating justice. *GeneWatch* (2004) **17**:3-9.
25. Shorett P. Technologies of justice. *GeneWatch* (2003) **16**:43-4.

26. Liptak A. You think DNA evidence is foolproof? Try again. The New York Times. 16-3-2003.
27. Meek J. DNA inventor rejects database plan. The Guardian. 3-5-2001.
28. Thompson WC, Taroni F, Aitken CGG. How the probability of a false positive affects the value of DNA evidence. *Journal of Forensic Science* (2003) **48**:47-54.
29. Brenner CH and Inman K. Commentary on: How the probability of a false positive affects the value of DNA evidence. *Journal of Forensic Science* (2004) **49**:192-3.
30. Mueller defends crime lab after questionable DNA tests. USA Today. 1-5-2003.
31. Burkeman O. US uproar at sloppy DNA tests. The Guardian. 12-3-2003.
32. Parson W and Steinlechner M. Efficient DNA database laboratory strategy for high throughput STR typing of reference samples. *Forensic Science International* (2001) **122**:1-6.
33. Thompson WC, Ford S, Doom T, Raymer ML, and Krane DE. Evaluating forensic DNA evidence: Essential elements of a competent defence review (2003) The Champion. **16**. Washington DC, USA: National Association of Criminal Defence Lawyers.
34. Walsh SJ, Moss DS, Kliem C, Vintiner GM. The collation of forensic DNA case data into a multi-dimensional intelligence database. *Science and Justice* (2002) **42**:205-14.
35. Disabled man turns down payment offer. ThisisWiltshire.co.uk 15-8-2000.
36. Williams R, Johnson P and Martin P. Genetic information and crime investigation (2004) London: The Wellcome Trust.
37. Pascali VL, Lago G, Dobosz M. The dark side of the DNA database. *The Lancet* (2003) **362**:834.
38. Kennedy, H. We should be outraged by these DNA databases. The Guardian. 14-5-2001.
39. The Home Office. New police powers to bring criminals to justice. 4-4-2004.
www.homeoffice.gov.uk/n_story.asp?item_id=908
40. House of Lords Select Committee on Science and Technology. Written evidence from the Forensic Science Service (2000) pp 39-44. London: The Stationery Office.
41. Strutt M. DNA down under. *GeneWatch* (2003) **16**:15-16.
42. Council of Europe. Convention for the protection of human rights and fundamental freedoms (2003) European Court of Human Rights.
www.echr.coe.int/Convention/webConvenENG.pdf
43. Asplen CH. International perspectives on forensic DNA databases (2003) ISRCL Conference, The Hague August 2003.
44. Jeffery S. Police seek DNA record of everyone. The Guardian. 8-9-2003.
45. Kennedy H. Stop taking uncivil liberties with DNA. *New Scientist*. 20-3-2004.
46. Beware of Big Brother state, warns data watchdog. The Times. 16-8-2004.
47. Scheeres J. Fears about DNA testing proposal. Wired News. 31-3-2003.
www.wired.com/news/politics/0,1283,58270,00.html
48. Liberty. Casualty of war: 8 weeks of counter-terrorism in rural England (2003) London: Liberty.
49. US turns back Brits. The Guardian. 8-3-2003.
50. Constans A. Applied Bio and Orchid target forensics labs. The Scientist. 2-2-2004.
51. Gill P, Werrett DJ, Budowle B, Guerrieri R. An assessment of whether SNPs will replace STRs in national DNA databases. *Science and Justice* (2004) **44**:51-3.
52. McKeown B. The next genetic revolution (2002) London: Genetic and Law Conference.
53. McKie R. Mobile DNA labs set to change face of sleuthing. The Observer. 2-5-2004.
54. Radford T. Over the counter gene analysis. The Guardian. 14-9-2002.
55. Fowler R. DNA the second revolution. The Observer, Supplement pp 50-5. 27-04-2003.
56. Factsheet: Commonplace characteristics (2002) London: The Forensic Science Service

57. Ananthaswamy A. Under the skin. New Scientist pp 34-7. 20-4-2002.
58. Lowe AL, Urquhart A, Foreman LA, Evett IW. Inferring ethnic origin by means of an STR profile. *Forensic Science International* (2001) **119**:17-22.
59. Cyranoski D. Japan's ethnic crimes database sparks fears over human rights. *Nature* (2004) **427**:383.
60. Sturm RA, Teasdale RD, Box NF. Human pigmentation genes: Identification, structure and consequences of polymorphic variation. *Gene* (2001) **277**:49-62.
61. Grimes EA, Noake PJ, Dixon L, Urquhart A. Sequence polymorphism in the human melanocortin 1 receptor gene as an indicator of the red hair phenotype. *Forensic Science International* (2001) **122**:124-9.
62. Flanagan N, Healy E, Ray A, Philips S, Todd C, Jackson IJ *et al*. Pleiotropic effects of the melanocortin 1 receptor (MC1R) gene on human pigmentation. *Human Molecular Genetics* (2000) **9**:2531-7.
63. Sykes B and Irven C. Surnames and the Y chromosome. *American Journal of Human Genetics* (2000) **66**:1417-19.
64. Munafo MR, Clark TG, Payne E, Walton R, Flint J. Genetic polymorphisms and personality in healthy adults: A systematic review and meta-analysis. *Molecular Psychiatry* (2003) **8**:471-84.
65. Laville S. Global DNA test narrows hunt for serial rapist. The Guardian. 28-4-2004.
66. Adams D. Can your DNA reveal where you're from? The Guardian. 6-5-2004.
67. Will profit kill forensic science? BBC News. 9-6-2004.
http://news.bbc.co.uk/1/hi/uk/3757049.stm
68. Cohen, N. If it works, sell it. The Observer. 30-11-2003.
69. The UK Biobank. UK Biobank. (2004). www.ukbiobank.ac.uk/
70. Booth N. Sharing information electronically throughout the NHS. *BMJ* (2003) **327**:114-15.
71. Mathieson SA. Image problem. The Guardian. 20-11-2003.
72. The Home Office. Legislation on identity cards: A consultation (2004) London:The Stationery Office.
73. Travis A. MPs say the case is made, but call for proper scrutiny. The Guardian. 30-7-2004.
74. Big Brother database. The Guardian. 31-7-2004.
75. Johnson P and Williams R. Post-conviction DNA testing: The UK's first 'exoneration' case? *Science and Justice* (2004) **44**:77-82.
76. The Home Office. Policing: Modernising police powers to meet community needs (2004) London:The Home Office.
77. Lehrman S. Prisoners' DNA database ruled unlawful. *Nature* (1998) **394**:818.
78. Plomin R. Genetics and general cognitive ability. *Nature* (1999) **402**:C25-C29.
79. Billings PR, Beckwith J, Alper JS. The genetic analysis of human behaviour: A new era? *Social Science and Medicine* (1992) **35**:227-38.
80. Wertz DC. Crime genes: The Danish adoption studies. GeneSage. 1-11-1996.
www.geneletter.com/archives/danishcrime.html
81. House of Commons. Hansard. Columns 344W, 345W, 17-3-2004.
82. The Home Office. The Home Office Strategic Plan 2004-2008. pp 32-3 (2004) London: The Home Office.
83. Cowan R. Home abusers 'likely to commit other crimes'. The Guardian. 20-3-2004.
84. Police National Computer. The Police Information Technology Organisation. 18-6-2004.
www.pito.org.uk/what_we_do/police_national_computer
85. Home Office. PNC Data Accuracy Project: Annex D Data Quality Final Report, CRB (2001) London: Home Office.

86. Association of Chief Police Officers. Code of Practice for Data Protection. (2002) London: ACPO.
87. Home Office. Sir Michael Bichard's Recommendations. (2004) London: Home Office. www.homeoffice.gov.uk/docs3/bichard_recommendations.html
88. Human Genetics Commission. Personal genetic information in forensic databases: Whose hands on your genes? A discussion document on the storage, protection and use of personal genetic information (2001) pp 43-7. London: Department of Health.
89. UK man DNA tested for swearing. Northern Echo. 26-2-2002.
90. Friends of the Earth. The Newbury bypass year review (1996) London: Friends of the Earth. www.foe.co.uk/archive/newbury/brief.html
91. National Union of Journalists. Photographers sue police, win money (2004) NUJ. www.nuj.org.uk/inner.php?docid=178
92. Phillips C. and Brown D. Entry into the criminal justice system: A survey of arrests and their outcomes (1998) London: Home Office.
93. Muir H. Met's DNA trawl sparks anger. The Guardian. 16-6-2004.
94. Guillen M, Lareu MV, Pestoni C, Salas A, Carracedo A. Ethical-legal problems of DNA databases in criminal investigation. *Journal of Medical Ethics* (2000) **26**:266-71.
95. Keating G. California DNA plan draws ire of civil libertarians. Yahoo News. 22-12-2003. news.yahoo.com/news?tmpl=story&u=/nm/20031223/pl_nm/crime_database_de
96. Bosch X. UN agency sets out global rules for protecting genetic data. *The Lancet* (2003) **362**:45.
97. Human Genetics Commission. Minutes of the HGC plenary meeting of 11 February 2004 (2004) London.
98. Booth J. Witness told in court he has HIV. The Guardian. 25-5-2004.
99. Taylor D. Worried police refuse to give DNA samples. The Express. 27-3-2004.
100. House of Commons. Hansard. Column 209W. 8-4-2003.
101. Police Association of Tasmania. DNA: Provision of samples by members. Association Newsletter March. 2002.
102. Liberty. Whose hands on your genes? Response to the Human Genetics Commission's discussion document on the storage, protection and use of personal genetic information (2001) London: Liberty.
103. Lin Z, Owen AB, Altman RB. Genomic research and human subject privacy. *Science* (2004) **305**:183.

GeneWatch UK

Printed by Interlith (Derby) Ltd, Unit 4 Dinting Lane Industrial Estate, Glossop SK13 7NU