DNA databases and human rights

GeneWatch UK

January 2011

Using DNA to trace people who are suspected of committing a crime has been a major advance in policing. When DNA profiling is used wisely it can help to convict people who have committed serious crimes or exonerate people who are innocent. However, concerns arise when individuals' tissue samples, computerised DNA profiles and personal data are stored indefinitely on a DNA database. There are concerns that this information could be used in ways that threaten people's individual privacy and rights and that of their families.

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

In some countries, databases that used to contain records only from people convicted of serious crimes are being expanded to include many innocent people who have been arrested but not convicted and people convicted or given police warnings or other sanctions for minor crimes. These people are treated as a 'risky population' who may commit future offences. In other countries, a DNA database of the whole population is proposed. Data-sharing, involving the transfer of information across international borders, is also on the increase.

Anyone who can access an individual's forensic DNA profile can use it to track the individual or their relatives. Access to a DNA sample can reveal more detailed information about a person's health. DNA evidence is not foolproof and mistakes can be made in laboratories or in court. However, there are currently no international safeguards that would protect people's privacy and rights and prevent miscarriages of justice.

This briefing is intended to provide people with the information that they need in order to understand how DNA databases are built and used and the implications for their rights. Its starting point is that safeguards are needed and that ordinary citizens should have a say in how these safeguards are developed.

It describes:

- How DNA databases are built, by the collection and retention of DNA samples and computer records
- Their role in solving crimes
- Expansions in uses
- The implications for privacy and human rights

- Impacts on children, ethnic minorities and other vulnerable people
- Safeguards that can be adopted

What is special about DNA?

DNA is a chemical that occurs inside every cell of a person's body. The DNA is contained in 22 pairs of structures known as chromosomes, shaped like an X, plus an extra pair – the sex chromosomes – which determine whether someone is male or female. In this final pair, women have two X chromosomes, but men have one X and one Y chromosome. Each chromosome consists of two long strings of chemical letters, twisted together in the famous shape of the double-helix. The chemical letters occur in pairs as rungs on this twisted chemical ladder. The four chemical letters of the genetic code spell out instructions to the cell about how to make the proteins that allow the human body to grow and function normally. The parts of the DNA sequence that contain the instructions for making proteins are known as genes.

DNA is useful to identify an individual because everyone's genetic code is thought to be unique, unless they have an identical twin. The string of chemical letters in a person's DNA can therefore act like a unique bar code to identify them. Because a person inherits half their DNA from their mother and half from their father, it can also be used to identify their relatives. Close relatives have a DNA sequence that is more alike than distant relatives or than someone who is unrelated.

Biological identifiers such as DNA, fingerprints, iris scans and digital photographs are known as 'biometrics'. In recent years there has been a lot of interest in developing biometrics to track and identify individuals as they enter or leave different countries or as they use public or private services, such as banks, computers, workplaces or hospitals.

Unlike iris scans and photographs, DNA and fingerprints can be left wherever a person goes: for example, on a glass or cup that they have been drinking from. This means that they can be used to track individuals – i.e. to find out whether they have been at a particular place, such as a crime scene or meeting place – where there might not be a scanner or a camera.

DNA differs from fingerprints in two main ways:

- Because DNA has a biological function, some of the information in a person's DNA may be relevant to their health or other physical characteristics, such as their eye colour.
- Because DNA is shared with relatives, a person's DNA can be used to help identify their parents or children and perhaps more distant relatives.

However, DNA profiles used by the police are not based on the whole sequence of someone's DNA, but only on parts of it. This means that the information contained in them is more limited than that contained in a person's whole genetic make-up.

What role can DNA play in solving crimes?

People can leave traces of their DNA at a crime scene because it is inside every cell of their body. DNA can be extracted from blood, semen, saliva or hair roots left at a crime scene using a chemical process. Tiny amounts of DNA can sometimes be extracted

from a single cell – such as cells shed from someone's skin when they touch an object – using new sensitive techniques (known as 'low copy number' DNA).

Police can also collect biological samples from suspects, usually by scraping some cells from inside their cheek.

When biological samples are collected by the police from a crime scene or an individual, they are sent to a laboratory for analysis. The laboratory extracts the DNA, amplifies it using a chemical reaction, and creates a string of numbers based on part of the sequence of chemical letters: this is known as a DNA profile. The DNA profile is not based on the whole sequence of the DNA (which would currently be very expensive) but on parts of it known as 'short tandem repeats' (STRs), where the chemical letters of the DNA are known to be repeated a different number of times in different people. The final DNA profile consists of a string of numbers based on the number of repeats at each of the STRs, plus the results of a test of the sex of the person from whom the sample came.

DNA profiles are not unique but the probability that two people's DNA profiles match by chance is low. If the DNA profile from an individual matches the DNA profile from a crime scene it is therefore highly likely (but not certain) that the blood, semen or saliva left at the crime scene came from them.

If the police have a number of suspects for a crime a DNA match can help them to identify who was at the crime scene and who wasn't. The value of this evidence in solving the crime will vary: DNA on a cigarette butt could have been dropped earlier in the day or have been planted by someone who wanted to implicate an innocent person in the crime; in contrast, DNA in semen from a woman who has been raped can show that a particular man was or was not likely to have been involved. However, even a rape case may not be straightforward: for example, if the man argues that the woman agreed to have sex.

When DNA samples are collected at a murder scene, many DNA matches will occur with DNA from the victim or with others who may have been there earlier in the day, not with the perpetrator of the crime. However, these matches can still help to provide important clues that will help to solve the crime. For example, a DNA match between the victim's blood and a blood stain on someone's shoes or clothes might be part of the evidence that leads to a criminal's conviction. In this example, a DNA database is not required because the victim's DNA can be obtained easily from him or her.

How does a DNA database help to solve more crimes?

Because a DNA profile is a string of numbers it can be stored on a computer database. If there is a group of known suspects for a crime, a DNA database is not needed to help the investigation. Any DNA profile collected from the crime scene can be compared directly with the DNA profiles of all the suspects to find out which one it comes from. However, a DNA database can be useful to bring new (unexpected) suspects into an investigation if there are no known suspects, or if the crime scene DNA does not match anyone who has already been identified.

A DNA database is a computer database containing records of DNA profiles. Usually there are two different sources of these DNA profiles: crime scene DNA samples and

individuals' DNA samples. When a new crime scene DNA profile is added to the database it is searched against all the other DNA profiles stored on the database. The crime scene profile might match with stored DNA profiles from other crime scenes, indicating a link between these crimes. Or it might match with an individual's DNA profile, suggesting that they could be a suspect for the crime. When a new DNA profile from an individual is added to the database it is searched against all the stored crime scene DNA profiles on the database. Again, a match may indicate that the individual may be a suspect for the crime. This process is known as 'speculative searching' and it results in reports of matches that can be sent back to the police for further investigation.

Although DNA can undoubtedly be useful to exonerate the innocent, a database of individual DNA profiles (as opposed to crime scene profiles) is never necessary to exonerate an innocent person, since this can always be done by comparing the DNA profile of the innocent suspect directly with the crime scene DNA profile. The Innocence Project in the USA has helped free a number of innocent people – including many on death row – by ensuring that crime scene DNA evidence is analysed and used correctly. However, individuals who have been wrongly convicted of a crime do not need their DNA profile to be on a database in order to be exonerated: their DNA profile can be taken from them at any time provided the relevant crime scene evidence has been retained.

When a match report is sent to the police they will need to do further work to use the information to try to solve the crime. The 'added value' of putting individuals on the Database is only to introduce new suspects into a past or future investigation. This depends on the number of 'cold hits' (unanticipated DNA matches) and the extent to which these matches lead to successful prosecutions. Matches with known suspects do not require a database, although they do require the ability to collect and use DNA during an investigation.

Stored DNA profiles are useless to the police unless some information about where they came from is also kept. Crime scene DNA profiles must be stored with information about when they were collected and where they came from, or linked to databases which contain this information by a crime reference number. The type of information that is stored with an individual's DNA profile will typically include their name and some other information about their appearance, suspected crime, and when the sample was taken. The individual's record on the DNA database may also be linked to other records on different databases, such as the record of their arrest, which can also include more personal data to make it easier for the police to track them down. A unique bar code can also be used to link the computer record containing the DNA profile back to the original DNA sample, stored in a laboratory.

Some countries keep databases only of crime scene DNA profiles, but others also keep databases of individuals' DNA profiles. If only DNA profiles from crime scenes are stored, a new individual's profile can still be searched against all *past* crime scene profiles to see if they are a suspect for any of these offences. However, retention of individuals' DNA profiles allows them to remain suspects for any *future* crime. The largest databases of individuals' DNA profiles are in the UK and USA which each store the DNA profiles of about 5 million people. Currently, laboratories in both these countries also store individuals' DNA samples linked to the person's record on the database.

What are the concerns about DNA databases?

The retention of DNA profiles and samples taken from *crime scenes* can be readily justified because they might be useful if an investigation needs to be re-opened in the future (either to convict a perpetrator, or to exonerate an innocent person). The major human rights concerns relate to the widening of the group of *individuals* (not crime scene samples) from whom DNA can be taken and then *retained*. This is because:

- DNA can be used to track individuals or their relatives, so a DNA Database could be misused by Governments or anyone who can infiltrate the system;
- In order to be useful to track suspects, DNA records are linked to other computer records such as records of arrest, which can be used to refuse someone a visa or a job, or lead to them being treated differently by the police;
- DNA samples and profiles contain private information about health and genetic relationships (including paternity and non-paternity).

Expanding DNA databases to include many persons who have merely been arrested represents a significant shift in which the line between guilty and innocent is becoming blurred. It undermines the presumption of innocence by treating people who have merely been arrested as somehow less innocent than others who have not been convicted of any offence. DNA databases also shift the burden of proof because people with records on them may be required to prove their innocence if a match occurs between their DNA profile and a crime scene DNA profile at some point in the future.

DNA is not foolproof so procedures need to be in place to ensure that matches between individuals' DNA profiles and stored DNA profiles do not result in miscarriages of justice. The more DNA profiles that are compared the more likely errors are to occur, and problems can also result due to poor laboratory procedures, failure to require corroborating evidence, or if DNA evidence is planted at a crime scene.

These concerns are exacerbated by wider problems within many criminal justice systems, which may result in racial, religious or political bias in whose DNA and personal information is kept, or insensitivity to the impacts on vulnerable people, including children and the mentally ill.

The benefits of DNA databases in solving crimes must be weighed against these downsides. The main issues are outlined in more detail below.

DNA databases, privacy and human rights

DNA is left at crime scenes, but it is also left elsewhere. The retention of DNA and fingerprints from an individual on a database therefore allows a form of biological tagging or 'biosurveillance', which can be used to attempt to establish where they have been.

This means that DNA databases can be used to track individuals who have not committed a crime, or whose 'crime' is an act of peaceful protest or dissent. For example, in a state where freedom of speech or political rights are restricted, the police or secret services could attempt to take DNA samples from the scene of a political meeting to establish whether or not particular individuals had been present.

Paper-based databases of individuals' records have been a powerful force in facilitating oppressive regimes and genocide, from the Nazis and the Stasi to Rwanda. DNA

databases link searchable computer records of personal demographic information, such as name and ethnic appearance, with the ability to biologically tag an individual and track their whereabouts using their DNA profile. An individual's relatives may also be identified through partial matching with their DNA. Thus, DNA databases significantly shift the balance of power from the individual to the state.

These concerns do not relate solely to the storage of DNA profiles and samples, but also to the other information that may be kept. For example, if DNA is collected on arrest and retained indefinitely, there is additional information kept in the police records of arrest and in the samples which may be stored in the laboratories which analysed them. The former may be accessed to assess someone's suitability for a job or visa, leading to potential erosion of their rights purely as a result of being arrested, even if they have not been convicted by a court. The latter contain additional personal information, such as whether someone is a carrier for a genetic disorder, that could be accessed and revealed if the sample is re-analysed.

Concerns about 'biosurveillance' extend beyond the state to anyone who can infiltrate the system and obtain access to an individual's DNA profile. This might include organised criminal or terrorist groups, or anyone seeking to track down an individual. For example, individuals on witness protection schemes may have their appearance altered but cannot change their DNA. If someone becomes suspicious about them and collects their DNA, their identity could be revealed by matching this to a stored DNA profile on a database, if this is accessible and linked to their old identity. Their relatives might also be found through 'familial searching' (looking for partial matches with the DNA profiles of other people on the database). Children who have been separated from an adult for their own protection could also be tracked down by someone with access to a DNA database if the adult has a sample of their DNA (taken from an old toothbrush, for example), or who shares part of their DNA profile because they are related to them.

Expansion in uses: familial searching, research uses and counter-terrorism

Familial searching is a process by which investigators look for partial matches between crime scene DNA profiles and the DNA profiles of individuals stored on a DNA database. This can be used to identify a relative of the suspect who can then be interviewed, potentially leading to the suspect's identification and perhaps a successful prosecution. Familial searching leads to a long list of partial matches which must be shortened by additional DNA testing and/or other policework. It has been pioneered in the UK, where it has helped to solve a number of serious crimes. However, it raises additional concerns about the privacy of individuals who are not suspects but who may be related to a suspect. In particular, instances of non-paternity might inadvertantly be revealed through the process of familial searching. If used routinely, familial searching could lead to significant abuses by allowing investigators or anyone who infiltrates the database to track down the relatives of political dissenters or to pursue enemies or identify paternity and non-paternity for personal, commercial or criminal reasons.

DNA databases consist of collections of biological samples (if stored), computerised DNA profiles and other information (such as criminal history and ethnicity) that may be valuable to genetic researchers. However, much research in this area is contentious due to the history of eugenics. In particular, attempts to link genetic characteristics to discredited concepts of race or to identify 'genes for criminality' are controversial. Unlike databases set up for research purposes, forensic DNA databases contain data collected

without consent and/or sometimes with consent for policing purposes only. Any attempt to use such databases to draw inferences about genetic characteristics is therefore in breach of established ethical standards. Such breaches have already occurred with some existing databases.

The use of DNA databases in criminal investigations requires an individual's identity to be revealed only if there is a match between their DNA profile and a crime scene DNA profile. Until recently, uses of DNA databases were restricted largely to looking for matches with crime scene DNA profiles. However, this is now changing. For example, in the UK DNA collected and retained under the Counter-Terrorism Act 2008 can now be used for "*identification…of the person from whom the material came*". This is a recent change of use which allows biological surveillance of certain individuals (i.e. the ability to use an individual's DNA to track and identify them, whether or not they are suspected of committing a crime). Clearly this may be useful to security services but it is also potentially open to abuse. UK Government proposals to collect DNA and fingerprints routinely on arrest for any offence (including dropping litter and parking fines) and use them routinely for identification purposes (i.e. by matching the individual to their details on the DNA and fingerprint databases, using facilities set up in shopping centres for such purposes) were dropped in 2008 following public outcry. However, this remains a potential use for DNA databases in the future, particularly as new technology develops which may allow on-the-spot DNA real-time testing and matching with database records.

A variety of techniques to predict individual characteristics from a DNA sample (hair, eye and skin colour and surnames) are also under development, with a view to identifying individuals who do not have a record on a DNA database. Scientific opinions differ on the likely value of such techniques, due to their fairly limited predictive value.

DNA is not foolproof

False matches between an individual's profile and a crime scene DNA profile can occur by chance, or due to poor laboratory procedures, and the implications of someone's DNA being at a crime scene can also be misinterpreted.

The chance of a false match between an individual's DNA profile and a crime scene DNA profile depends on the system of DNA profiling that is used. The standards used to create a DNA profile have changed with time and vary from country to country: the US uses 13 STRs at different places in the genetic sequence, but most other countries use fewer STRs. The UK system (which uses 10 STRs) is estimated to have about a 1 in a billion 'match probability': this is the likelihood that an individual's DNA profile matches a crime scene DNA profile by chance even if the DNA at the crime scene did not come from them. Although this likelihood is very low, the number of false matches that occur depends on the number of comparisons that are made between different DNA profiles. If every crime scene DNA profile is compared against every stored DNA profile on a large database by speculative searching, a small number of false matches are expected to occur simply by chance. False matches are more likely to occur with relatives, as the brother or cousin of someone who has committed a crime will share some of their relative's DNA sequence. This problem is exacerbated if some crime scene DNA profiles are not complete, as the likelihood of a false match can then increase considerably.

The quality of DNA profiles taken from a crime scene can vary according to the source of the DNA, whether it has become degraded over time, and whether the DNA is a mixture

from more than one person. Tiny samples of DNA from a single cell are more prone to errors in analysis and can also be easily transferred to a crime scene, even if an individual was not present. In contrast, a large quantity of blood found at the scene of a murder or burglary can give very reliable results. A mixture can be interpretated in many ways since there is no clear way to tell which part of the profile comes from which individual: this means that mixed DNA profiles are open to interpretation, particularly if a forensic laboratory is biased by trying to find a match with a particular suspect. Many DNA profiles taken from crime scenes are not complete or contain mixtures of more than one person's DNA: this increases the likelihood of a false match with the wrong person.

As the size of a DNA database increases the number of false matches is expected to increase: this can waste police time following false leads, and lead to potential miscarriages of justice.

DNA samples can also be wongly analysed or mixed up during laboratory procedures, resulting in a match with the wrong person if quality assurance procedures are not followed.

Comparing DNA profiles from different countries can be complicated by the fact that not all countries test STRs at the same places along the DNA. This means that the crime scene DNA profile and the individual's DNA profile can often be compared at a smaller number of places that would usually be the case, leading to a higher likelihood that a false match will occur by chance. Routine cross-border speculative searching of crime scene DNA profiles against stored DNA profiles from individuals arrested in other countries is therefore likely to throw up many more false matches than if such searches are restricted to one country or limited to only a small number of profiles.

Even if a DNA match is genuine, a person's presence at a crime scene may not mean that they committed the crime. The weight attached to the match should depend on whether there is additional corroborating evidence: as well as the potential for false matches there may be a credible alternative explanation for the person's presence at the crime scene, or the DNA evidence could have been planted. Using speculative searching to identify suspects can mean that the balance of evidence is shifted: the onus is on the individual to prove they did not commit the crime, rather than the other way around. Any individual with a record on a DNA database may also be vulnerable to being falsely implicated in a crime by the planting of evidence: by corrupt police officers, powerful government agencies, or by criminals. Even if a miscarriage of justice does not occur, an individual who is falsely accused of a crime as a result of a DNA match may be subjected to a stressful police inquiry, pre-trial detention, or extradition to a foreign country.

Racial bias, mass screens and impacts on children and vulnerable people

In many countries, ethnic minorities are more likely to be arrested and prosecuted for criminal offences. DNA databases often include disproportionate numbers from such minorities and therefore the impacts on their privacy and rights may be greater than on others. Records on DNA databases, or linked records on police databases, often contain information about ethnicity. Records of names can also be searched for typical surnames associated with a particular country of origin or religion, and the computer records of such individuals can therefore be identified. This opens the possibility of such records being used to facilitate discrimination – restricting access to jobs, visas or

housing - or more serious abuses of human rights, including ethnic cleansing and even genocide.

DNA samples may also be requested during an investigation on a voluntary basis. This may be necessary for example to check that a DNA profile from the crime scene is not that of the victim or of friends or relatives with a legitimate reason to be present. Sometimes this process is extended to mass screens of everyone living in a particular area, in an attempt to narrow down an investigation. There have been many instances in the US and UK where such 'DNA dragnets' have been racially targeted, people have been coerced into taking part and/or their records have been kept on databases without their consent following the investigation. Mass screens are rarely effective unless there is a specific reason to test a specific group of people (for example, the suspect is known to work in a particular office) and they can lead to loss of trust in policing in targeted communities.

People who are mentally ill and children are often arrested for minor offences. If their DNA is taken routinely on arrest (as has happened in England and Wales since 2004) their privacy and rights can also be disproportionately affected. Vulnerable individuals can find having their DNA taken and their records kept particularly disturbing and some individuals have even become suicidal as a result. Stigmatising children and young people for minor crimes or on the basis of false accusations can also be counter-productive: some evidence suggests that this may make them more likely to commit offences in the future.

A good use of police resources?

DNA is undoubtably a valuable tool in criminal investigations and has helped to catch the perpetrators of some very serious crimes, including rapes and murders. However, the idea that there would be no more rapes or murders if everyone had their DNA profile recorded on a database is totally mistaken. In addition to concerns about privacy and rights, the main limitations to this idea are: (i) the difficulties in collecting relevant and useful crime scene DNA evidence; (ii) the very low likelihood of most people committing serious crimes for which DNA evidence might be relevant; (iii) the costs and practical difficulties associated with collecting and keeping reliable computer records of DNA profiles and associated information from large numbers of people; (iv) the impacts on public trust in policing.

For example, in England and Wales a major government project to expand the use of DNA began in 2000. Positive benefits were achieved by improving the collection of DNA from crime scenes and speeding up its analysis. However, there were still real practical limits in how much useable DNA could be collected in this way: despite improvements in procedures, DNA profiles are still loaded to the DNA database from less than 1% of recorded crimes. Many crime scenes do not reveal any useable DNA, or may include DNA from multiple passers-by. Thus there will always be a real practical limit to how many crimes can be solved using DNA.

More importantly, a massive increase in the number of individuals' DNA profiles collected and stored on the DNA database in England and Wales did not increase the likelihood of being able to prosecute someone for a crime. This appears to be because DNA profiles were collected and stored from too wide a pool of people (everyone arrested for any offence which the police keep records of, regardless of whether they

were ultimately charged or convicted). The likelihood of any of these individuals committing a crime for which DNA evidence was relevant was very low, so most of these stored profiles did not help to solve any crimes. The inclusion of hundreds of thousands of innocent people's records on the DNA database also resulted in a loss of public trust in policing. Although it is difficult to quantify the impacts, this may have made some crimes more difficult to solve by making some people less cooperative with police investigations. In Scotland, stricter rules on the retention of DNA profiles maintained public support and Scotland's DNA database remained an effective tool in criminal investigations despite most innocent people's records being deleted.

In 2010, putting someone's DNA profile on the database in England and Wales was estimated to cost £30 to £40 (USD 46-62) and storing one person's DNA sample cost about £1 (USD 1.54) a year. Running the computer database itself cost £4.29 million (USD 6.6 million) in 2008/09 and additional unknown policing costs were associated with crime scene examination and the police time spent taking DNA and fingerprints from people who had been arrested. If DNA were to be collected from the whole population, rather than only from people who have been arrested, this would obviously cost substantially more and also raise practical and ethical difficulties about how to collect DNA from everyone without consent. Collecting DNA from foreign visitors would add further to the costs and difficulties and could have negative impacts on people willing to travel to the country. Collecting DNA from babies at birth would raise serious ethical issues about consent and the role of the medical profession. Large databases of children's DNA profiles together with their contact information would be attractive to abusers or to anyone wishing to establish paternity or non-paternity.

In addition, bigger databases – and more comparisons between DNA profiles stored in different countries - increase the likelihood of false matches, as described above. These can waste police time following false leads, even if they do not lead to miscarriages of justice.

This means that, rather than bigger databases being better, there is a trade-off between the pros and cons: restrictions on whose DNA is collected and stored are needed if a database is to be cost-effective. The main benefits of DNA in criminal investigations apear to have been delivered by: improving the collection and analysis of crime scene DNA (including the number of crime scenes visited and the speed and quality of the analysis of samples); ensuring that known suspects for a crime have their DNA analysed and compared with relevant DNA evidence in a way that does not misrepresent the value of this evidence in court; and retaining the DNA profiles of repeat offenders. Reanalysing evidence from old crime scenes has also helped to correct some serious micarriages of justice.

Safeguards and standards

Different ethical, legal and technical standards are set for DNA databases in each country. Important questions include:

- Under what circumstances should the police be allowed to collect DNA and store samples and profiles?
- Are there any procedures to destroy individuals' samples or records when they are no longer needed?
- What data is sent to whom and is it kept securely?

- What technical standards must be met by the DNA profiles before they are loaded to the database?
- Are quality assurance procedures being followed in the labs that analyse the DNA?
- How are DNA matches used in court and is corroborating evidence needed?
- Can the database and samples be used for additional purposes other than solving crimes?
- Is there any independent oversight and information about how the database operates?
- Are safeguards included in legislation, or only in guidelines that can easily be changed?

Some of the relevant issues are considered in more detail below.

Collection of DNA

Most DNA samples collected by the police are taken without consent, usually using a mouth swab whilst the individual is in police custody. In such circumstances, the police may be allowed to use 'reasonable force' if someone refuses to give a sample. A DNA sample can be taken without consent by pulling a few hairs from the person's head: the hair roots, but not the hair itself, contain their DNA.

One important safeguard is legislation that restricts the collection of DNA by the police without consent to circumstances where it is necessary for solving crimes, and where the interference with a person's rights is not disproportionate to any benefit that might be achieved. There is a wide range of views in different countries about whan DNA should be collected by the police. Issues include:

- Should the DNA be directly relevant to the crime for which an individual has been arrested, or can DNA be taken just to search an individual's DNA profile against stored DNA profiles from other crimes?
- If DNA can be taken when it is not needed for a specific investigation, are there other restrictions on when it should be collected (depending, for example, on the seriousness of the alleged offence, whether the individual has been charged or merely arrested, or their age or other circumstances)?
- Should there be any independent oversight for these decisions, should they be left to the discretion of the police, or should DNA collection be routine if certain conditions are met so that everyone is treated fairly?

Additional safeguards are needed for people who give their DNA to the police on a voluntary basis during the course of an investigation: their consent to this should be fully informed and freely given, without coercion from the police or others.

DNA analysis and reporting

DNA may be sent to police or commercial labs for processing. Data security and privacy policies are critical to ensure that private information is not revealed to unauthorised persons during processing, or accessed by someone who wants to infiltrate the system.

Laboratory quality assurance procedures are essential if people are not to be falsely accused of crimes due to sample mix-ups or poor quality DNA profiles. New procedures,

such as procedures to interpret very small samples of DNA or mixed DNA samples also need careful independent evaluation.

Data loading and match reporting

Procedures need to specify: the DNA profiling system to be used; how complete a DNA profile needs to be before it can be uploaded to the Database; and reporting requirements for matches with partial DNA profiles.

Reporting procedures to the police and to the courts need to ensure both privacy and reliability of the information that is provided. Investigators also need to understand the limitations of the technology and how and why it can be misinterpreted.

Retention of DNA profiles, samples and other data

Because of the impacts on privacy and human rights, one of the most contentious issues has been the question of when biological samples, DNA profiles and other police records can be retained.

Some countries, such as Germany, destroy each individual's DNA sample as soon as the computerised DNA profile that is needed for identification purposes has been obtained from it. This protects privacy by preventing the sample from being re-analysed to obtain personal health information. However, other countries retain samples, in some cases indefinitely.

A separate question is how long individuals' DNA profiles and other personal information should be stored on computer databases. Most countries with DNA databases keep the DNA profiles of people who have committed serious crimes such as rape and murder on the database indefinitely, but there are a wide variety of rules for entering and removing people who are convicted of more minor crimes.

When DNA databases were first set up, DNA profiles, samples and police computer records were legally required to be deleted and destroyed if someone was acquitted or charges against them were dropped. In England and Wales the law was changed in 2001 to allow the indefinite retention of all this information, but in December 2008 the European Court of Human Rights found unanimously that this practice was in breach of the European Convention on Human Rights. The law in England and Wales has not yet been changed, although the new Government has promised to implement the judgment.

Safeguards are also needed to ensure that people who have given their DNA voluntarily during an investigation should not be entered into databases or have their data retained against their will.

Access to and uses of stored data and samples

Access to DNA samples and to the DNA database must be restricted to a small number of authorised persons if security breaches are not to occur.

Uses of DNA database records and samples should also be restricted. Key issues include:

- When speculative searches of the database can be made;

- Under what circumstances DNA profiles from overseas can be searched against a database and how decisions are made to exchange data internationally;
- Whether and under what circumstances 'familial searches' of a database can be made (looking for partial matches with the DNA profile of a relative);
- Whether the database can be used for research purposes and if so, whether research on people's genetic characteristics can take place without their consent;
- Whether the database can be used for the identification of individuals who are not suspects for a crime.

Use of DNA evidence in court

A key issue is whether prosecution requires corroborating evidence, or whether a person can be convicted on the basis of DNA evidence alone. The process of explaining DNA evidence to the court is also crucial: the value of DNA evidence can easily be overstated by using misleading statistics, particularly when the crime scene DNA profile is not complete. Expert forensic witnesses must not be under pressure to misrepresent evidence in cases where the interpretation may be in doubt (for example, when a mixed DNA profile is involved).

Another important issue is whether extradition or transfer of suspects to other countries can take place on the basis of a DNA match alone.

Oversight and governance

Legislation and policies can only safeguard privacy and rights and prevent miscarriages of justice if there is sufficient scrutiny of whether policies are being properly implemented and what the outcomes are. This requires independent oversight as well as the regular publication of public information about the size, costs and effectiveness of the database in solving crimes.

The impacts of a DNA database on privacy, human rights and justice will also depend on the context in which it operates, i.e. on the integrity of the criminal justice system in the country as a whole.

Conclusions

DNA databases raise important issues about privacy and human rights. Safeguards are essential because:

- DNA can be used to track individuals or their relatives, so a DNA Database could be misused by governments or anyone who can infiltrate the system;
- In order to be useful to track suspects, DNA records are linked to other computer records such as records of arrest, which can be used to refuse someone a visa or a job or otherwise discriminate against them;
- DNA samples and profiles contain private information about health and genetic relationships (including paternity and non-paternity).

Essential safeguards include legal restrictions on the circumstances in which DNA and associated information can be collected and retained.

DNA is not foolproof, so procedures also need to be in place to ensure that misleading interpretations of DNA evidence do not result in miscarriages of justice.

GeneWatch UK
60 Lightwood Road, Buxton, Derbyshire, SK17 7BB
Phone: 01298 24300
Email: mail@genewatch.org Website: www.genewatch.org
Registered in England and Wales Company Number 3556885