the policefoundation
improving policing for the benefit of the public

# The briefing

Series 1, Edition 5 – April 2009


Photo courtesy of Home Office


© Dra Schwartz/Istock


© Mark Evans/Istock

# The use of DNA in forensic policing

This Police Foundation Briefing looks at the use of DNA in forensic policing and identifies some of the key issues which arise from its use.

## Introduction

Forensic science is usually defined as the application of natural sciences to the resolution of legal conflicts. Its founding principles can be traced back to 19th century scientists such as Edmund Locard, who was the first to coin the phrase 'every contact leaves a trace'. The use of forensic science in criminal investigations began in the late 19th century when fingerprints were first used to identify suspects, particularly at crime scenes, and to this day about one in ten fingerprints found at crime scenes result in a match(1).

The modern equivalent of fingerprints is DNA. Its use constitutes the biggest change in forensic investigation techniques since the advent of fingerprinting and has stimulated considerable controversy and debate. But, like fingerprints, DNA is not a panacea in the fight against crime and to fully understand its

limitations as well as its usefulness, it is important to describe what exactly DNA is and how it contributes to forensic criminal investigations before setting out the legal framework governing its use and some of the issues and controversies associated with it.

### What is DNA and how is it used?

Deoxyribonucleic Acid (DNA) is a complex biological molecule that contains all the necessary information for an organism to function, as well as the information required for its development and procreation. DNA samples are the genetic information derived from the biological material taken from an individual. There are two kinds of DNA samples: 'intimate' (pubic hair, semen, etc.) and 'non-intimate' (mouth swab, hair, etc.).

DNA found at the scene of a crime, such as blood, saliva or semen, may be visible or invisible, in a liquid or dried state, and can be found anywhere – on the ground, walls, objects, or clothes. This means that samples can often be contaminated, either by another person's DNA, or by chemical and biological agents, reinforcing the need for DNA to be pure and of good quality for it to be useful in police investigations. Following its extraction, the DNA quality is assessed, and if it is found to be satisfactory, a DNA profile can be determined from it and subsequently loaded onto the National DNA Database (NDNAD).

While DNA samples remain the property of the police force that provided them, they are kept and stored by the company that extracted the DNA profile from the samples. Only six companies in the UK are approved to provide the NDNAD with DNA profiles from suspects or crime scene samples. They are accredited both by the United Kingdom Accreditation Service and the Custodian of the NDNAD.

The structure of DNA was discovered by James Watson and Francis Crick in 1953, but DNA analysis has only been used as a forensic technique since the beginning of the 1980s. The Royal Commission on Criminal Procedure (1981) first considered the technique in relation to police powers over suspects and detainees, stating that 'only people who have raised a reasonable suspicion in the minds of the police should be subject to coercive powers' and rejected the use of non-consensual sampling(2). Since then, the law relating to the taking of samples, including issues relating to consent, storage, intimate and non-intimate samples, and the persons subjected to sampling, has undergone numerous and sometimes very important changes.

## The legal framework

The law governing DNA sampling for analysis was set-up by the Police and Criminal Evidence Act (PACE) 1984, and its codes of practice. This legislation sets out the definition of intimate and non-intimate samples, the persons authorised to take samples and the circumstances where consent is required. The latter comprises reasonable grounds for believing that the detainee was involved in a serious arrestable offence and that the sample would confirm or disprove such involvement. Non-intimate samples (such as non-pubic hair, or footprints) can be taken by a police officer without a person's consent, whereas intimate samples (such as saliva or semen) can only be taken by a dentist or a doctor following approval by a police superintendent.

In 1993, the Royal Commission on Criminal Justice recommended a widening of the definition of 'serious arrestable offence' to include assault and burglary, and the adoption

of a less restrictive definition of 'non-intimate' samples as introduced in Northern Ireland five years earlier to counter the threat of terrorism. These recommendations were subsequently implemented through the Criminal Justice and Public Order Act 1994 (CJPOA), which went further than the Royal Commission by replacing 'serious arrestable offence' with 'any recordable offence'(3). The police were given the power to arrest a suspect who refused to provide a sample and Section 63 allowed for 'speculative searching' of the database, which some commentators saw as the first step towards the creation of the National DNA Database(4).

In 2001, the Criminal Justice and Police Act removed the obligation to destroy DNA samples following an acquittal or when proceedings have been dropped. Other changes included the diminishing of the level of the authorising officer in the case of intimate samples from superintendent to inspector, and in the case of non-intimate samples, nurses could now do the sampling instead of doctors. Most subsequent developments followed this general trend of extending the circumstances in which samples could be taken and kept, and of loosening the requirements for taking such samples: the Police Reform Act 2002, for example, authorised other health-care professionals to take intimate samples.

In 2003, the Criminal Justice Act amended section 63 of PACE, and allowed the taking of non-intimate samples, without consent, upon arrest, for any recordable offence. It meant that samples could be taken upon 'reasonable suspicion' for an offence, irrespective of whether the sample could prove guilt or whether it would be used in the investigation, and be kept indefinitely on the NDNAD and therefore used in speculative searches. This led to a jump in the number of DNA samples taken from individuals and stored on the NDNAD from around 800,000 in 1999/00 to just under 4 million in 2005/06(5).

***In the case of S and Marper the Court ruled that 'the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences...fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard'.***

The Counter-Terrorism Bill currently going through Parliament will, if passed unamended, lead to a further increase in the number of individuals on the NDNAD since it will enable the linking of the NDNAD to databases held by MI5 and MI6 on the grounds of 'national security' (and in particular the retention of DNA samples for individuals on control orders)(6). However a recent ruling from the European Court of Human Rights has halted the trend towards increasingly taking and storing DNA samples from unconvicted individuals. In *S and Marper*, the Court ruled that 'the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences...fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard'(7). This ruling will force the government to alter its policy, either by imposing a limit on the length of time DNA samples and profiles can be kept, and/or by deleting the DNA samples and profiles of individuals not convicted, or convicted of a minor offence.

# The use of DNA in forensic investigations

The aim of forensic investigation is to reveal the source of biological evidence collected at the scene of a crime(8), which usually entails comparing a DNA profile from an individual to a DNA profile from that scene. This can be done either by checking a scene of crime profile against a database of individual DNA profiles, or against the DNA profile of a known police suspect. This can sometimes be problematic, since DNA at a crime scene is often found in a degraded state, having for example been exposed to weather conditions for a sustained period of time, or to caustic chemicals, which affect the 'quality' of the DNA. The amount of DNA found may also be extremely small, requiring careful handling in specific conditions to minimise the risk of cross contamination. DNA sampling from individuals is more straightforward: samples are usually of one type; they are collected under controlled conditions, with professional supervision, and are properly stored. If anything goes wrong, the samples can usually be re-collected.

The use of DNA in criminal investigations requires the assistance of forensic scientists, who are responsible for the collection, sampling, analysis, and storage of DNA. It is important that the police understand the problems inherent in the collection and analysis of DNA. Equally, forensic scientists need to understand the nature of a criminal investigation in order to collect and analyse the right samples efficiently and according to the requirements of the law.

Until the 1950s, police officers carried out the majority of routine-trace evidence gathering at the scene of a crime. In 1966, specialist Scene of Crime Officers (SOCOs) were introduced by the Home Office and since then, SOCOs have been civilianised in order to free up police time. Around 3% of the police force in any given Basic Command Unit (BCU) is engaged in forensic work, almost half of which are SOCOs(9).

***It is important that the police understand the problems inherent in the collection and analysis of DNA. Equally, forensic scientists need to understand the nature of a criminal investigation in order to collect and analyse the right samples efficiently and according to the requirements of the law.***

There are five basic stages where forensic support is needed: attending the crime scene, transporting the evidence, analysing the evidence, obtaining identification, and finding a match. The decision relating to whether or not to attend a particular crime scene can be a difficult one, and there is no clear correlation between the scenes of crimes most attended and identification rates: while theft from a motor vehicle is only attended to, on average, in 25% of cases, there is a 47% DNA identification rate. Burglaries, on the other hand, only result in a DNA identification in 36% of cases even though SOCOs are extremely likely to attend the crime scene(10).

The identification of DNA does not equate to a detection, however. For burglaries, the average detection rate is around 50%, while for theft of a motor vehicle it stands at around 75%. While police forces have a large amount of discretion in choosing how to proceed with a case, this discretion is not the only factor in deciding what the next step should be. Research has shown that in the cases where a DNA match was found but no action was taken, the main reasons for this decision were: advice from the Crown Prosecution Service (25%), problems of legitimate access (that is

to say, the DNA came from people who had legitimate access to the scene of crime) (30%), and lack of further evidence (14%). In 31% of cases, the reasons were unclear(11).

The quicker the scene is examined, the more chances there are of a detection. The whole process, from investigating the scene to arresting a suspect takes on average about two months: one day to attend the scene, 12 days to transport the recovered material to the centre, 15 days to analyse the samples, five days to arrive at identification, and 31 days to arrest and detain a suspect. It seems as though it is the latter stage of the process that can be most effectively reduced: a 2004 Home Office performance improvement work package, designed to maximise the effectiveness and efficiency of the forensic process, should be implemented in all UK Scientific Support Units(12).

## How helpful is DNA in solving crime?

Proponents of the NDNAD point out that it has been an invaluable tool in the fight against crime. Although DNA is only effective in solving 0.4% of all recorded crime(13), figures show that, in 2006-07 alone, this amounted to 40,000 crimes, either as a direct result of a DNA match, or through a development subsequent to a DNA match(14). The usefulness of DNA is, however, most prominent in certain types of crimes, such as burglary. The normal detection rate for burglary is around 17%, but this rises to 40% when DNA is detected at the scene(15). The equivalent figures for theft from motor vehicles are even more impressive at 9% and 60% respectively(16). It is also argued that as technology progresses, the number of cases where DNA can be retrieved and used will increase, and that the usefulness of DNA in fighting crime is therefore exponential as technology progresses(17).

## The use of DNA: key issues

There is a danger in assuming that using DNA evidence is somehow "objective", or that it covers the uncertainty of police work with a cloak of scientific objectivity. If prejudice is employed in selecting evidence in the field, or in deciding which piece of evidence to submit for research and analysis, then the final result will be biased. It is also dangerous if the police rely too heavily on DNA evidence. There may be many reasons why DNA is found at a particular location, and sometimes it cannot be ascertained whether the initial contact that led to DNA being left at the scene of crime was major or minimal. If DNA is found at a scene which is a public place, it might not mean very much at all: a person's DNA can be deposited on another individual through contact, such as a handshake, who himself would transfer that same DNA to another location, for example, by touching a wall. DNA evidence is therefore not a 'silver bullet', nor is it sufficient to charge a suspect without further supporting evidence(18).

While DNA is usually sampled from arrestees for matching with a crime scene sample and speculative searches against the NDNAD, there are other ways in which DNA is sampled. Targeted intelligence screening, for example, which involves the mass screening of a whole population group within a designated area, was used in 1987 in a rural part of Leicestershire to help solve a series of rape cases. Two rapes had occurred within the area and DNA showed that one individual was allegedly responsible for both rapes. Despite a confession, DNA tests showed that the suspect was in fact not responsible for the rapes. The police proceeded to take DNA samples from all men aged between 16 and 34 from three local villages, a total of 5,500

samples. Whilst none of them returned a match, it was later brought to the attention of the police that one man had given a sample on behalf of a work colleague. Both men were arrested, and the DNA of the person who had not submitted his own sample was found to match DNA found at both crime scenes. The suspect was convicted of the rapes a year later.

Mass screenings are however ethically problematic. If a number of individuals refuse to comply, should the police have the power to arrest them? If a single individual out of thousands refuses to comply, an arrest might be considered feasible, but if one hundred refuse, it becomes problematic. In practice, this would result in non-compliance becoming a *de facto* criminal offence, which contradicts the notion that an arrest can only be effected if there is "reasonable suspicion" that an individual has committed a crime. There is also the issue of trust between the public and the police to consider; one of the key principles underpinning British policing, the notion of policing by consent, could be damaged by the impression that the police are misusing their power to take and store the DNA of large numbers of innocent individuals.

## The National DNA Database

The UK's National DNA Database is, relative to its population, the biggest database of its kind in the world with around 5.1 million DNA profiles(19). It contains four kinds of samples: scene of crime (SOC) samples; casework samples taken from suspects for comparison with a SOC sample in a specific case; criminal justice (CJ) samples; and volunteer samples. Every new profile loaded onto the database is checked against all other profiles already on the database. When a subject profile is loaded, the match can either be with a SOC profile, or against another subject profile, indicating that the individual's profile is already on the database. When a SOC profile is loaded, the match can either be to a subject profile, thereby identifying a potential suspect, or to another SOC profile, thereby linking different crimes together but without identifying a suspect. Following a match, the information from the database is passed to the relevant unit in the police force that submitted the enquiry, who will then pass on this information to the investigating officer. A 'DNA match' indicates that a subject profile loaded onto the database matches a SOC profile already on the database. A 'DNA detection' indicates that the crime has been recorded as 'cleared-up' by the police. Around half of DNA matches lead to a DNA detection(20).

While the NDNAD started out as an intelligence database only, its role and size expanded rapidly following the DNA Expansion Programme announced in September 1999. The aim of the Expansion Programme was to input a DNA profile for all known active suspect offenders, with a target of loading 3 million samples onto the database by April 2004(21). Prior to the introduction of the Expansion Programme, an average of 200,000 DNA profiles were added to the database every year but after September 1999, this increased to around 500,000 per year between 2001 and 2005, and to around 700,000 since 2005(22). This programme, coupled with the legislative changes designed to facilitate the circumstances in which DNA samples could be taken from individuals, largely explain the rapid growth and current size of the NDNAD.

## Regulation and oversight

The NDNAD, including all the DNA samples and the information derived from them, is currently owned by the National Policing Improvement Agency (NPIA). The Database itself is governed by the NDNAD Strategic Board, which comprises representatives from the Association of Chief Police Officers (ACPO), the Forensic Science Service (FSS), the Home Office and the Human Genetics Commission(23). A NDNAD custodian unit in the Home Office is responsible for setting the standards of performance for forensic science laboratories who want to provide DNA profiles to the NDNAD and for ensuring that these are achieved and maintained.

The Forensic Science Service (FSS), which became a Government-owned Company (GovCo) in December 2005, is contracted by the Government to provide operational services for the NDNAD. This contract, which is overseen by the Home Office, requires the FSS to receive and load profiles onto the NDNAD and search it for matches. Their work is now scrutinised by an Ethics Group, created by the Government to provide Ministers with independent ethical advice on the operation and practice of the database.

The regulation of the database has been criticised, however, for being too easy to ignore or to overrule, often because of strong political pressure. Data collected for purposes other than solving crime (e.g. by phone companies and ISPs) has subsequently been used by the police under the Regulation of Investigatory Powers Act and the Data Retention Directive(24). A recent case should ensure that that regulation of the use of DNA is tighter(25).

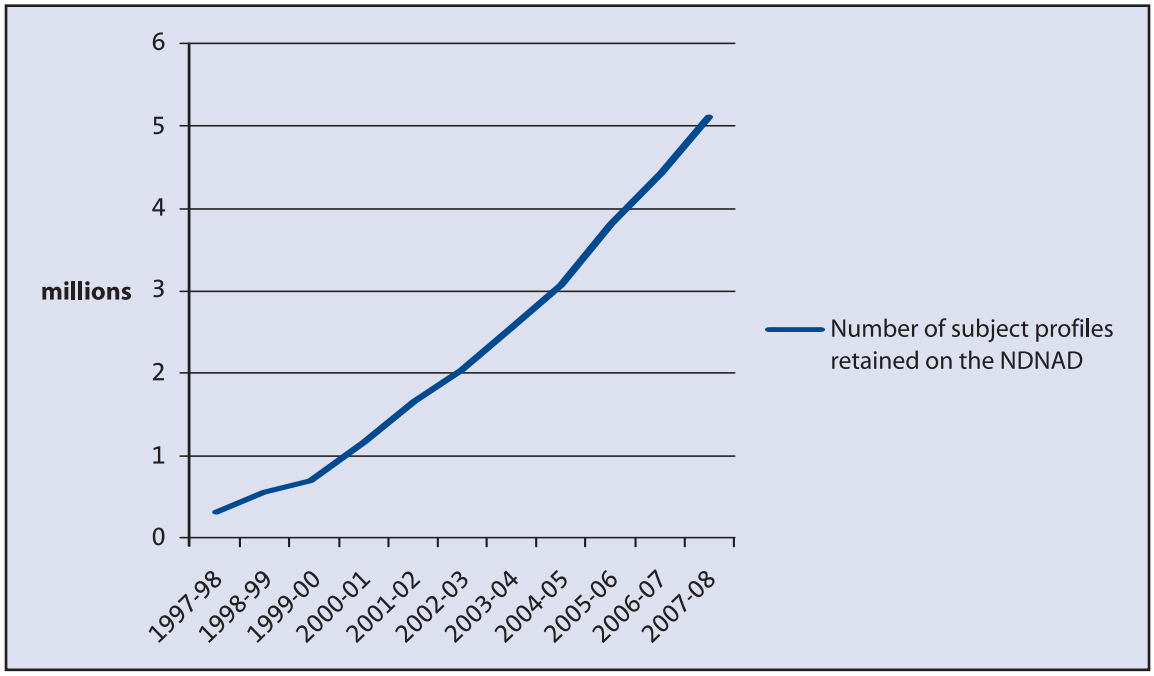
## Some key issues relating to the NDNAD

The establishment and evolution of the NDNAD has proved more controversial than the use of DNA in forensic investigations. The debate has mostly centred on the breadth of the database, its efficiency, and on ethical issues such as the use of DNA samples for research purposes, the permanent retention of samples, and the use of familial searches.

Following the DNA Expansion Programme, the NDNAD now comprises nearly 4 million individual subject profiles and over 400,000 SOC sample profiles(26). Keeping the DNA profiles of criminals convicted of a serious offence on the database is not too controversial, and this framework is the one adopted by most European countries as well as most US states. Since approximately 50 percent of all crimes are committed by a hardcore of 100,000 criminals(27), keeping their details on the NDNAD seems like an effective strategy.

The rationale behind keeping the DNA profiles of individuals who have been arrested for an offence but later released or acquitted (around 800,000 according to some commentators(28)) is that the effectiveness of the database is proportional to the number of profiles in it: the higher the number of profiles, the higher the chances of a match from a crime scene. This claim, however, does not seem to be substantiated: despite the number of individual profiles almost doubling between 2002-03 and 2006-07 from around 2 million to almost 4 million (see fig. 1), the percentage of recorded crimes for which there is a DNA detection has remained constant, at around 0.37%(29). Significantly, the chance of a crime scene DNA profile matching an individual's profile on the DNA Database is higher in

Fig. 1. Number of subject profiles retained on the NDNAD since 1997




The National DNA Database Annual Report 2006/07, Home Office 2007

Scotland than in England and Wales, even though in Scotland most people have their records removed from the database on acquittal(30).

Critics have complained that keeping the profiles of innocent individuals on the NDNAD has created an arbitrary list of 'permanent suspects'. The recent ruling from *S and Marper* in the European Court of Human Rights, however, could force the UK to move towards a more limited database, where profiles are either kept for a specific amount of time depending on the offence an individual was arrested for, or one where individuals not convicted of an offence can have their DNA record permanently deleted from the database on request.

It is also argued that the make-up of the database is problematic in itself, irrespective of the legal status of the individuals on it(31).

There are about a million individuals on the database whose DNA profiles were added when they were children or young adults (i.e. under 18) and around half a million people had their DNA profiles added when they were under 16 years old(32). About 300,000 of those added as children are still under 18(33). Also, certain ethnic groups are disproportionally represented on the database: about 30% of the entire UK black population aged over 10 has their DNA profile on the database(34). The proportion is much higher for young black men: in 2007, Baroness Scotland confirmed to the Home Affairs Committee that three-quarters of the young black male population would soon be on the DNA database(35).

It has also been argued that both the permanent storage of DNA samples and the speculative searching of DNA profiles breaches privacy laws(36). Privacy has already been eroded through the expansion of CCTV,

the retention of fingerprints, GPS technology, tracking on the internet, or even systems such as Google Earth. In the words of Sun Microsystems Chairman and CEO Scott McNealy, "You have no privacy, get over it."(37). It has been advocated that to protect privacy in the long-term, the amount of data that is collected should be minimised(38).

While a DNA profile is only a sequence of numbers, algorithms are now being developed by computer scientists that will enable them to reveal new information from previously-held data(39). Apart from allowing individual DNA profiles to be matched, the database does not reveal any other information apart from gender, however this could change in the near future(40). Systems of cryptography which could prevent an individual or company from obtaining personal information from a DNA profile do exist, and there is a strong argument for applying those systems to the NDNAD(41).

Issues also arise from the storage of DNA samples by private companies and their possible use in controversial research(42). DNA samples contain unlimited genetic data, including health-related material and information about who may be related to whom, so there are real concerns about who has access to them, particularly since the Home Office is accepting applications for the use of the DNA database for studies not directly linked to preventing crime(43). Facilitating research concerned with identifying an individual's genetic predisposition or attempts to find a 'criminal gene' is highly contentious, as is research undertaken for commercial purposes, especially since the individuals concerned will not have consented to their DNA being used in this way.

Finally, there are the risks that governments might lose the information contained on the database or that a malignant government could one day use this information to the detriment of its citizens. The former seems well-founded in light of recent incidents such as the loss of CDs containing the personal details of 25 million child benefit claimants(44).

## What happens in other countries?

Most countries use DNA in forensic investigations and standardisation of the use of DNA and of databases could one day become an important issue in the international fight against crime. However the extent to which other countries have developed sophisticated databases for the storage and analysis of DNA samples varies considerably. In Scotland, DNA may be taken on arrest for any imprisonable offence and computerised DNA profiles and samples are kept permanently if the individual is convicted. However, in May 2006, the Scottish Parliament voted against the permanent retention of DNA from innocent people. Instead, police powers were expanded to allow temporary retention (for up to 5 years) from a much smaller number of people who had been charged but acquitted of a serious, violent or sexual offence.

In the USA, each state is responsible for its own DNA database, as well as setting down the conditions for its use (although the FBI has its own meta-database which combines all the states' databases). Only four states allow for the involuntary taking of samples from arrestees – California, Texas, Louisiana and Virginia. The respective statutes in Louisiana, Texas and Virginia require that the permanent retention of records on the DNA database is dependent upon a guilty verdict, and so a record should be expunged on acquittal or dismissal(45). Only California authorises the inclusion of a DNA profile from a suspect indicted for an offence, but not convicted.

In most EU countries (such as France, Netherlands, Germany, Austria and Finland), DNA samples and profiles are deleted from the database if the suspect is acquitted or not prosecuted(46). The largest database in the EU after the UK is in Austria, which contains under one percent of its population. In Sweden, only DNA samples of criminals who have spent more than two years in prison are recorded. In Norway and Germany, court orders are required to retain data, and only in the case of serious offences, or where an individual is likely to re-offend. Portugal, however, has plans to introduce a DNA database of its entire population.

## Conclusion

The use of DNA in forensic investigation has proved to be as revolutionary as the discovery of fingerprints. Further technological advances will, in all likelihood, improve the reliability and utility of DNA, enabling the recovery of DNA traces from extreme conditions or places. But it is important to understand that DNA is not and probably never will be a 'silver bullet'.

The future of the DNA database, and in particular the extent to which it is used to retain data on innocent people, and if so for how long, will now depend on how the Government responds to the ruling of the European Court of Human Rights. It seems likely that it may decide to delete the DNA samples of individuals who were neither charged nor convicted of a serious or sexual offence. In those cases where the government does keep samples, a time limit of, say, five years is likely to be imposed, after which samples must be destroyed. The Government may also relax the conditions under which individuals can have their record deleted from the database. Whilst these changes are substantial, they should not significantly weaken the police's ability to catch serious criminals.

Considering the scientific advances which now enable the identification of information from limited DNA profiles, it seems likely that new ways of protecting the privacy of DNA profiles will need to be found(47). Safeguards governing the use, storage, retention and transport of DNA samples as well as any research conducted upon them will be very important. This could be achieved by creating an independent, transparent and accountable governing body, thereby preventing the risk that companies might one day access the database in order to undertake controversial genetic research.

Ways of ensuring that the database is not discriminatory or used for malevolent purposes may also need to be considered, such as introducing safeguards, strengthening regulation and oversight and perhaps addressing the issue of discrimination in the criminal justice system as a whole. Further questions are likely to be raised about the ownership of DNA. While it is conceivable that individuals convicted of a serious offence should lose their right to keep their DNA private, it's another matter to expect innocent individuals to accept the same.

## References


1. McCartney, C. (2006) *Forensic Investigation and Criminal Justice*, Willan Publishing
2. HMSO (1981) *Royal Commission on Criminal Procedure* (The Phillips Commission), (Cmnd 8092), para 3.128, HMSO
3. HMSO (1988) *Hansard*, HC (Series 5) vol. 135, col 650, HMSO
4. McCartney, C. (2006) *Forensic Investigation and Criminal Justice*, Willan Publishing
5. Home Office (2007) *The National DNA Database Annual Report*, *2006/07,* Home Office
6. Available at: http://services.parliament.uk/bills/2007-08/counterterrorism.html
7. S. and Marper v. the United Kingdom – 30562/04 [2008] ECHR 1581 (4 December 2008)
8. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge
9. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge; Newburn, T. Williamson, T. and Wright, A. (2007) *Handbook of Criminal Investigation*, Willan Publishing
10. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge.
11. Newburn, T. Williamson, T. and Wright, A. (2007) *Handbook of Criminal Investigation*, Willan Publishing
12. Newburn, T. Williamson, T. and Wright, A. (2007) *Handbook of Criminal Investigation*, Willan Publishing
13. GeneWatch UK (2006) *The DNA Expansion Programme: Reporting Real Achievement?* February 2006, GeneWatch UK
14. Home Affairs Committee, Second Report, found at: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhaff/181/18102.htm
15. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge
16. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge.
17. *Advancing Justice Through Forensic DNA Technology*, Subcommittee on Crime, Terrorism and Homeland Security of the House of Representatives, July 2003
18. Newburn, T. Williamson, T. and Wright, A. (2007) *Handbook of Criminal Investigation*, Willan Publishing
19. Home Office (2007) *The National DNA Database Annual Report*, *2006/07,* Home Office
20. GeneWatch UK (2006) *The DNA Expansion Programme: Reporting Real Achievement?* February 2006, GeneWatch UK
21. McCartney, C. (2006) *Forensic Investigation and Criminal Justice*, Willan Publishing
22. Home Office (2007) *The National DNA Database Annual Report*, *2006/07,* Home Office
23. Home Office (2007) *The National DNA Database Annual Report*, *2006/07,* Home Office
24. See Attorney General's Reference No 3 of 1999
25. London Borough of Lambeth v S, C, V, & J (No 3) in the Family Division of the High Court, 2006
26. Home Office (2007) *The National DNA Database Annual Report*, *2006/07,* Home Office
27. Home Office (2004), *Home Office Strategic Plan*, Home Office
28. Hansard 15 Sep 2008 : Column 2070W
29. GeneWatch UK (2008), *The National DNA Database: Q&A,* updated May 2008, GeneWatch UK
30. GeneWatch UK (2008) *Ten Myths about the DNA Database*, GeneWatch UK
31. Leapman, B. 'Three in four young black Men on the DNA database', *Sunday Telegraph* 5 Nov 2006.
32. Hansard 20 Nov 2008: Col 723W
33. Hansard 27 Oct 2008: Col 677W
34. Hansard 10 Nov 2008: Col 800W
35. Home Affairs Committee, Second Report, found at: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhaff/181/18102.htm
36. GeneWatch UK (2007) *Police Retention of DNA*, February 2007, GeneWatch UK
37. San Francisco Chronicle (2003) 'On the Record: Scott McNealy',14 September 2003, SFGate.com

38. House of Commons Home Affairs Committee, 'A surveillance Society', Fifth Report of the Session 2007/08
39. Bohannon, P., Jakobsson, M. And Srikwan, S. (2000) *Cryptographic Approaches to Privacy in Forensic DNA Databases*, Public Key Cryptography
40. Bohannon, P., Jakobsson, M. And Srikwan, S. (2000) *Cryptographic Approaches to Privacy in Forensic DNA Databases*, Public Key Cryptography
41. Bohannon, P., Jakobsson, M. And Srikwan, S. (2000) *Cryptographic Approaches to Privacy in Forensic DNA Databases*, Public Key Cryptography
42. Home Office (2008) *National DNA Database Ethics Group Notes*, Home Office and see 'Genetic Research and DNA Storage', GeneWatch UK, found at: http://www.genewatch.org/sub-539491
43. Home Office (2008) *National DNA Database Ethics Group Notes*, Home Office and see 'Genetic Research and DNA Storage', GeneWatch UK, found at: http://www.genewatch.org/sub-539491
44. Harrison, D. 'Government's record year of data loss', *Daily Telegraph* 7 January 2008
45. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge.
46. Semikhodskii, A. (2007) *Dealing with DNA Evidence*, Routledge.
47. Bohannon, P., Jakobsson, M. And Srikwan, S. (2000) *Cryptographic Approaches to Privacy in Forensic DNA Databases*, Public Key Cryptography

**£3.50**