



Tania Simoncelli, Helen Wallace
Spiralling out of control

The UK has the world's largest DNA database, containing information on almost three million people, the estimated number of active criminals in the UK. Samples can be taken from anyone charged with any offence, even when DNA is not usually needed for the investigation - begging, for example, or taking part in a prohibited public demonstration. Meanwhile, the rest of the world is close on the UK's heels. While few would object to the use of DNA in criminal cases, the vast scale of data retention, compared to the relatively few cases in which DNA profiles actually lead to a crime being solved, creates misgivings about the potential misuse of data. The invasion of privacy is a particular issue where family members are scooped up in investigations without their knowledge or consent. Ethnic discrimination could also be exacerbated by life-long data retention: huge imbalances between the number of arrests black and white people in the US and the UK could lead to a situation where entire populations are DNA recorded.

The past decade has witnessed an extraordinary growth in DNA databases for use in criminal intelligence and health research. The databases range in size from a few hundred to a few million samples, with the UK at the scientific forefront.

The UK's National DNA Database (NDNAD) is the oldest, largest and most inclusive national forensic DNA database in the world. Now in its tenth year of operation, it contains DNA samples and profiles from more than 2.5 million individuals and is expected to expand over the next few years to include some 5 million people, nearly 10 per cent of the population. On file is DNA drawn from a wide range of criminals -- from violent offenders to those convicted of misdemeanours by way of others who have eventually been found innocent.

US advances have attempted to keep pace with the UK. Three years after NDNAD went live, the FBI began to operate its own national database and software system: the Combined DNA Index System (CODIS) enables local, state and national authorities to share DNA profiles electronically and contains more than 2.3 million offender DNA profiles. Since 1998, all 50 US states have actively collected DNA from people caught up in the criminal justice system; in 2004, they were connected by CODIS.

Meanwhile, the UK has developed the disturbing tendency to seek samples from an ever-widening range of individuals; it has also decided to collect and permanently retain DNA from people who are merely arrested -- and where the UK leads, the US and the rest are following as fast as may be.

The first DNA profiling technique was discovered in the UK in 1985; in the following year, research in the US led to more sensitive DNA profiling techniques. Successful use of the technology in criminal investigations

encouraged investment in further research and development in both countries. In 1994, the UK passed the Criminal Justice and Public Order Act, which enabled the police to take DNA samples without consent from anyone charged with any recordable offence; NDNAD went live the following year and police powers to take and retain DNA have expanded more or less ever since.

In 2000, Prime Minister Tony Blair announced the DNA Expansion Programme. This aimed to include "virtually the entire active criminal population" — an estimated 3 million people — by 2004 and has all but reached its target. Samples are now routinely taken and permanently retained from anyone who is arrested on suspicion of any recordable offence, including such things as being drunk in a public place, begging or taking part in a prohibited public procession. DNA evidence is usually not relevant to such investigations.

Development and expansion in the US went more slowly but by 1994 the DNA Identification Act had authorized the FBI to maintain a national database and develop its CODIS system. Most of the early US state statutes were explicitly limited to profiles from sexual offenders, but the past decade has witnessed a dramatic expansion. Today, 34 states collect DNA from all felons, 28 from juvenile offenders and 38 from those who commit some category of misdemeanour; four states, among them California, which from 2009 plans to collect DNA from all felony suspects, have moved beyond convicted criminals. Last year, a federal law expanded CODIS to allow states to upload DNA profiles of anyone convicted of or charged with any crime.

This expansion is likely to continue. In 2003 alone, 18 US states passed laws to include more categories of people in their databases. In addition, there have been at least two proposals to use DNA samples collected from newborns for medical and law enforcement purposes. In the UK, plans are under way to collect DNA samples from 500 000 adults for medical research and a proposal to collect DNA samples for health purposes from all newborns will be revisited in about five years. Samples in these collections would be linked to National Health Service records, a plausible "back door" entry for the government should it wish to establish a forensic database.

Meanwhile, DNA databases have gone global. Australia, New Zealand and most European nations have them; China and South Korea have plans to establish them. The government of Portugal recently announced that it would create the world's first universal forensic database and Interpol has gone international with a database that allows all member states to be notified of matches, though it limits access to the profile to the original policing agency.

One controversial use of DNA databases is "familial searching", which involves looking for "partial matches" between a crime scene profile and individual profiles on the database. Because close relatives share similar DNA profiles, law enforcement can track down close relatives of individuals identified by a partial match and ask for a DNA sample. First used in the UK in 2002, this method has since been used in at least 20 cases and helped solve five of them. The FBI's director has stated that his organization does not run this type of search. But at least two states, Massachusetts and New York, have regulations that explicitly allow it and most other state laws do not forbid it. So far, we know of no confirmed uses of familial searching in the US, although in one recent case in Kansas it was alleged that the police were led to a suspect by retrieving a DNA sample from the suspect's daughter.

Few people have problems with the use of DNA in criminal cases. The permanent retention of DNA in a database for use in future investigations is, however, another matter. An individual captured in a police database becomes an automatic suspect for all future criminal investigations in which database searches are used. This undermines the presumption of innocence that is central to many criminal justice systems.

Setting aside this fundamental problem, benefits of the use and expansion of these databases must be weighed against their social costs: while the temptation on the part of law enforcement is to put more people into the database, the practical benefits of expansion may be limited. In the UK, for example, despite the large number of people on the database, DNA profiles are obtained from the examination of less than 1 per cent of crime scenes. In 2002 and 2003, only 1.6 per cent of all crime detections were attributed to DNA database matches, including only 0.3 per cent of all detections for violent and sexual offences. At the same time, there are many reasons to be concerned about the use and expansion of police databases, including their impact on individual privacy, their potential for misuse by governments, discrimination and the possibility of error and wrongful conviction.

Unlike a fingerprint, DNA has the potential to provide information about health and relationships, including one's risk of having or developing a genetic condition. Many concerns about DNA collections stem from the permanent retention of the biological sample — a practice that is common to both UK and US databanks. The DNA profiles held on the database are usually sufficient for identifying a person and his/her relatives. They are unlikely to contain personal genetic information about health or other characteristics. DNA samples, however, contain virtually unlimited amounts of genetic information. In the UK, all DNA samples are currently retained indefinitely, linked to an individual's record on the database. In the US, samples can also be retained indefinitely, although some states require authorities to expunge DNA records upon reversals or convictions.

Law enforcement authorities in both countries have argued that sample retention is necessary for "quality assurance purposes". But re-testing the same sample clearly cannot correct many errors, including sample mix-ups. In fact, in both the UK and the US, testing of a fresh DNA sample from the suspect is always required before the DNA evidence is admissible. The UK government's advisory body, the Human Genetics Commission, has concluded that the reasons given for retaining samples are "not compelling"; although the UK Home Office recognizes that the retention of DNA samples is "one of the most sensitive issues to the wider public", it currently has no plans to change this practice.

The potential for misuse of stored DNA samples is real. It can reveal personal genetic or family information, or be wrongly acquired for controversial genetic research. Moreover, threats to genetic privacy extend well beyond the millions of people whose samples are currently on file because of the family overlap. Genetic research using the database is likely to be misleading as well as controversial.

In the UK, uses of the database are limited to crime detection and prevention but include controversial research such as attempts to predict ethnicity from DNA profiles. Because DNA samples are collected without consent, genetic research using the samples and/or database bypasses the usual safeguards, such as the need for informed consent from participants and review by an ethics

committee. Categories in the NDNAD such as "ethnic appearance" — as determined by a police officer — are meaningless for scientific purposes and the DNA profiles and samples will not be representative of either the general or "criminal" population.

Thirteen US state laws include a vague, open-ended authorization allowing the database to be used for "other humanitarian purposes"; Alabama, for instance, explicitly authorizes the creation and use of a DNA population statistical database "to provide data relative to the causation, detection and prevention of disease or disability" as well as to assist in educational or medical research.

The use of "familial searching" raises an additional privacy concern since it risks revealing cases of non-paternity or other relationships that may be unknown to the members of a suspect's family.

The dramatic expansion of UK and US databases, particularly the process of including people who have merely been arrested, has redefined the nature and purpose of these so-called "criminal" databases. Because DNA is such a powerful tool in tracing individuals, law enforcement databases could well be used as instruments of government surveillance.

The UK database now contains the first permanent list of those arrested since April 2004 along with their DNA samples and profiles. In the US, California's new law means that this year more than 600 000 people will qualify for testing, a ten-fold increase. From 2009, all of California's 425,000 annual felony arrests will qualify for testing; yet 60 per cent of these will ultimately not be convicted of any crime. Profiles from all those arrested and charged will also be uploaded into CODIS, even if they are eventually proved innocent. California will also retain suspect DNA — including that which is voluntarily provided during "DNA dragnets" or "mass screenings" — for up to two years. These DNA profiles can be "speculatively searched" for matches with DNA profiles from any number of investigations.

Expanding the databases puts an increasing number of unsuspecting people on a "suspect list" regardless of whether they have ever been charged or convicted. 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 proved guilty" and of rehabilitation. Without adequate protections, permanent records of arrest could be used to restrict people's rights and freedoms, making it difficult or impossible for them to obtain travel visas or employment.

Life-long retention of data is also likely to exacerbate discrimination against certain groups of people, particularly ethnic minorities. Racial bias permeates society and the criminal justice systems in both the UK and US. A study in California in the early 1990s revealed that an astonishing 92 per cent of the black men arrested by police on drug charges were subsequently released for lack of evidence or inadmissible evidence. In the UK, *New Scientist* magazine calculated that the DNA database now contains DNA profiles from nearly one third of black adult males, compared to only 8 per cent of white adult men.

Within living memory, both fascist and communist governments in Europe have used identity papers and personal records to oppress particular sectors of their populations. In the US, census records were used during World War II to round up and intern innocent Japanese-Americans. Since 11 September, 2001, many people of Arabic, Middle Eastern or South Asian descent have been

detained, arrested or harassed by government authorities. Some forensic scientists argue that the only way to prevent discrimination is to expand DNA databases to include whole populations.

Not that this will end discrimination generally, as recent attempts to use crime scene samples to predict the genetic ancestry of potential suspects indicates. Results for ancestry might be misleading and the genetics of predicting eye, skin or hair colour is extremely complex and poorly understood; the police might misinterpret the information they are given. Without better oversight, there is a danger that such tests will be used selectively to reinforce existing prejudices.

Despite what the media chooses to portray, DNA testing is not infallible. DNA samples can be switched or contaminated; analyses can be misinterpreted, especially when crime scene samples contain mixtures of DNA from more than one source or where DNA is degraded; and results can be mistakenly reported.

The fallibility of DNA testing was made painfully clear when, in January 2003, the Houston, Texas Police Department's crime lab was shut down following an investigation that revealed widespread problems including gross mishandling and misinterpretation of DNA evidence by laboratory personnel. Some 1300 cases are under review and, to date, one person, Josiah Sutton, has been released from prison after serving four years for a crime he did not commit. Errors are likely to multiply as databases expand, becoming the rule rather than the exception. Miscarriages of justice this far should caution us against too great a reliance on the wonders of the DNA database.

Published 2005-10-25

Original in English

Contribution by Index on Censorship

First published in *Index on Censorship* 3/2005

© Tania Simoncelli, Helen Wallace/Index on Censorship

© Eurozine