REVIEW ARTICLE

Current scenario of forensic DNA databases in or outside India and their relative risk

Sachil Kumar a,*, Anoop K. Verma b,1, Pratibha Singh b,2, Raghvendra Singh b,3

a Post Graduate Department of Pathology, King George’s Medical University UP, Lucknow, India
b Department of Forensic Medicine & Toxicology, King George’s Medical University UP, Lucknow, India

Received 21 January 2015; revised 3 February 2015; accepted 1 March 2015

Abstract DNA technology has proved to be a worthy investigative tool for releasing the innocent citizens and bringing forth the person responsible for serious crimes. In a populated country like India there is requirement for these types of databases. The Union government is working on a new version of a legislation that seeks to set up a national DNA database of ‘offenders’. As expected with the great success of the use of forensic DNA databases, new challenges are coming up. To rise to the challenges, different strategies have been proposed for increasing search capabilities, the implementation of which is on-going. The Federal Bureau of Investigation (FBI) in the US has proposed to add more autosomal short tandem repeat (STR) loci to its current core set of loci. The constant growth in the size of forensic DNA databases raises issues on the criteria of inclusion and retention and doubts on the efficiency, commensurability and infringement of privacy of such large personal data collections. People have difficulties that spill beyond the level of simple privacy and confidentiality issues.

© 2015 Hosting by Elsevier B.V. on behalf of The International Association of Law and Forensic Sciences (IALFS).

Contents

1. Introduction ........................................................................................................ 00
2. Current scenario in India ...................................................................................... 00
3. Benefits and risks .............................................................................................. 00
4. Privacy and human rights .................................................................................. 00
Source of funding ................................................................................................. 00

* Corresponding author. Mobile: +91 9412125533.
E-mail addresses: sachilvohra@gmail.com (S. Kumar), vermakgmc@gmail.com (A.K. Verma), pratibha.singh06@gmail.com (P. Singh), rupaniraja@rediffmail.com (R. Singh).
1 Mobile: +91 9415583355.
2 Mobile: +91 9795816559.
3 Mobile: +91 9795957555.

Peer review under responsibility of The International Association of Law and Forensic Sciences (IALFS).

http://dx.doi.org/10.1016/j.ejfs.2015.03.002

© 2015 Hosting by Elsevier B.V. on behalf of The International Association of Law and Forensic Sciences (IALFS).
1. Introduction

DNA technology has proved to be a worthy investigative tool for releasing the innocent citizens and bringing forth the person responsible for serious crimes. The motive of establishing forensic DNA databases was to develop investigative leads for solving crime and usually was the purview of “criminal justice agencies for law enforcement identification purposes”.

Forensic DNA databases are now well established in many countries in the world. The first government database (NDNAD) was set up by the United Kingdom in 1995 followed by New Zealand. France set up the Fichier National Automatisé des Empreintes Génétiques (FNAEG) in 1998. In the USA, the FBI has organized the Combined DNA Index System (CODIS) database. Originally intended for sex offenders, they have since then been extended to include almost any criminal offender.

In England and Wales, anyone arrested on suspicion of a recordable offence must submit a DNA sample, the profile of which is then stored in the DNA database as a permanent record. In Scotland, the law requires the DNA profiles of most people who are acquitted would be removed from the database. In Sweden, only the DNA profiles of criminals who have spent more than two years in prison are stored. In Norway and Germany, court orders are required, and are only available, respectively, for serious offenders and for those convicted of certain offences and who are likely to reoffend. Forty-nine states in the USA, all apart from Idaho, store DNA profiles of violent offenders, and many also store profiles of suspects.

In 2005 the incoming Portuguese government proposed to introduce a DNA database of the entire population of Portugal. However, after informed debate including opinion from the Portuguese Ethics Council the database introduced was of just the criminal for the population.

The United States maintains the largest DNA database in the world, with the CODIS holding over 9 million records as of 2011. The United Kingdom maintains the National DNA Database (NDNAD), which is of similar size. The size of this database and its rate of growth, is giving concern to civil liberties and political groups in the UK, where police have wide-ranging powers to take samples and retain them even in the event of acquittal. Other countries have adopted privately developed DNA databases, such as Qatar, which has adopted Bode dbSEARCH. In addition to direct matching between known and unknown sample profiles, profiles from missing persons and their relatives, as well as unidentified human remains, are included in a number of databases.

Missing person identification also is an invaluable module for investigating certain crimes. When a match is made from a national DNA database to link a crime scene to an offender who has provided a DNA sample to a database that link is often referred to as a cold hit. A cold hit is of value in referring the police agency to a specific suspect but is of less evidential value than a DNA match made from outside the DNA database. As of March 2011, 361,176 forensic profiles and 9,404,747 offender profiles have been accumulated, making it the largest DNA database in the world. As of the same date, CODIS has produced over 138,700 matches to request, assisting in more than 133,400 investigations. The United Kingdom National DNA Database consisted of an estimated number of 5,512,776 profiles of individuals as of March 2011.

The growing public approval of DNA databases has seen the creation and expansion of many states’ own DNA databases. California currently maintains the third largest DNA database in the world (naturally, as CODIS contains all states’ database information). Political measures such as California Proposition 69 (2004), which increased the scope of the DNA database, have already met with a significant increase in numbers of investigations aided. The application of DNA databases has been expanded into two controversial areas: arrestees and familial searching. An arrestee is a person arrested for a crime and who has not yet been convicted for that offence. Currently, 21 states have passed legislation that allows law enforcement to take DNA from an arrestee and enter it into the state’s CODIS DNA database to see if that person has a criminal record or can be linked to any unsolved crimes. In familial searching, the DNA database is used to look for partial matches that would be expected between close family members. This technology can be used to link crimes to the family members of suspects and thereby help identify a suspect when the perpetrator has no DNA sample in the database.

As expected with the great success of the use of forensic DNA databases, new challenges are coming up. The databases are experiencing rapid growth, and thus there is a potential of increased adventitious hits; the power for current and new applications (e.g., missing person identification and familial searching) requires additional infrastructure support; and there is an increased desire for international data sharing, which possibly could be retarded if only a relatively small number of loci is shared among laboratories worldwide.

2. Current scenario in India

In a populated country like India there is huge requirement for these types of databases which may help in stopping different types of fraud like Ration card fraud, Voter ID Card fraud, driving licence fraud etc. The database may help the Indian police to differentiate the criminals and non-criminals. The Union government is working on a new version of a legislation that seeks to set up a national DNA data base of ‘offenders’, that allows for the collection and storage of DNA samples of those accused in cases ranging from homicide, sexual assault and rape to even violations under the motor vehicle Act.

The initiative to draft a Bill regulating the use of DNA samples for crime-related reasons began in 2003, when the Department of Biotechnology (DoB) established a committee...
known as the DNA Profiling Advisory Committee to make recommendations for the drafting of the DNA profiling Bill 2006, which eventually became the Human DNA Profiling Bill 2007. The 2007 draft Bill was prepared by the DoB along with the Centre for DNA Fingerprinting and Diagnostics (CDFD). The CDFD is an autonomous institution supported by the DoB. In addition to the CDFD, there are multiple Central Forensic Science Laboratories in India under the control of the Ministry of Home Affairs and the Central Bureau of Investigation, along with a number of private labs which analyse DNA samples for crime-related purposes.

Activists have opposed the draft bill as a potential breach of citizens’ privacy, and have challenged it on ethical and technical grounds. Helen Wallace, a member of Gene Watch, a U.K.-based group advocating against DNA databases, feels that India must learn from international experiences, particularly from the U.K. which was the first country to set up a database in 1995 that even allowed retention of DNA records of innocent citizens. In May, the U.K. passed the Protection of Freedoms Act which will remove about 1 million records from the database.

In a controversial move that threatens to increase the intrusion by the state into the lives of ordinary citizens, the UPA government is set to introduce a DNA Profiling Bill in the winter session of Parliament. Once it becomes a law, the bill will grant the authority to collect vast amount of sensitive DNA data of citizens even if they are “suspects” in a criminal case. The data will be held till the person is cleared by court.

The bill has already raised the hackles of many groups working on privacy issues who are worried that if it becomes a law, it would empower the government to create intrusive databases. The bill proposes the creation of a national DNA data bank that will be manned by a manager of the rank of a joint secretary to the government of India. For activists, this will help the government assume the role of an alarming “Big Brother” collecting vast amount of sensitive data of citizens. The preamble to the bill admits that “DNA analysis offers sensitive information which, if misused, can cause harm to a person or society”. The government has also slipped in a section that allows for “volunteers” to give their DNA profiles which will be maintained. It is not clear under what circumstances the “volunteers” will share their sensitive data with the government.

The data, the bill states, will also be used for the “creation and maintenance” of population statistics and can be used for “identification, research, protocol development or quality control”. Strangely enough, the penalty for “misuse” of the DNA profiles attracts a mild imprisonment of a few months or a fine of a paltry Rs 50,000.

In fact, law enforcement agencies like the CBI (central bureau of investigation) have been pushing the government for an early enactment of the bill. They have cited the findings of a UK parliamentary report issued by its Office of Science and Technology in February 2006 that states that convictions in criminal cases went up drastically after the government agreed to maintain DNA profiling data in perpetuity. The report records that the detection of crime in the UK went up from 26% to a healthy 40% after DNA samples were loaded in the national DNA database.

However, since this kind of a database usually co-exists with crime statistics, there is a fear that members of minority communities could be easily targeted. This is a concern that has also been raised in the British parliamentary report which says that “blacks and ethnic minorities are disproportionately represented” in their database because more of them are arrested for alleged crimes. Currently, the present bill does not address these concerns of the inherent imbalance in racial profiling when maintaining a national DNA database.

Meanwhile, senior police officials who are familiar with the bill and have made extensive presentations to the DBT (Department of Biotechnology) are upset that the bill makes a provision for deleting the DNA profile data after a person has been acquitted by courts. They feel that maintaining the data and increasing it slowly and steadily will go a long way in preventing and solving crimes. While that is a legitimate argument, the absence of a strong privacy law raises concerns about the obtrusive nature of the proposed DNA Profiling Bill.

3. Benefits and risks

The constant growth in the size of forensic DNA databases raises issues on the criteria of inclusion and retention and doubts on the efficiency, commensurability, and infringement of privacy of such large personal data collections. In contrast to the past, not only serious but all crimes are subject to DNA analysis generating millions and millions of DNA profiles, many of which are stored and continuously searched in national DNA databases. As always when big datasets are gathered new mining procedures based on correlation became feasible. For example, “Familial DNA Database Searching” is based on near matches between a crime stain and a data based person, which could be a near relative of the true perpetrator. Again the first familial search was successfully conducted in the UK in 2004 and led to the conviction of Craig Harman of manslaughter. Craig Harman of Frimley, Surrey was convicted and jailed for six years on the basis of “familial DNA searching”, which linked him to the crime scene via a close relative’s DNA profile. The strategy was subsequently applied in some US states but is not conducted at the national level. It was during a dragnet that it first became public knowledge that the German police were also already involved in familial search strategies. In a little town in Northern Germany the police arrested a young man accused of rape because they had analysed the DNA of his two brothers who had participated in the dragnet. Because of partial matches between crime scene DNA profiles and these brothers they had identified the suspect. In contrast to other countries, the Federal Constitutional Court of Germany decided in December 2012 against the future court use of this kind of evidence. Alec Jeffreys early on has questioned the way UK police collects DNA profiles, holding not only convicted individuals but also arrestees without conviction, suspects cleared in an investigation, or even innocent people never charged with an offence. He also criticized that large national databases as the NDNAD of England and Wales are likely skewed socioeconomically. It has been pointed out that most of the matches refer to minor offences; according to GeneWatch in Germany 63% of the database matches provided are related to theft while <3% related to rape and murder. The changes to the UK database came in the 2012’s Protection of Freedoms bill, following a major defeat at the European Court of Human Rights in 2008. As of May 2013 1.1 million profiles (of about 7 million) had been destroyed to remove
innocent people’s profiles from the database. The government of Portugal in 2005 proposed a DNA database containing samples of all its inhabitants. Despite the threats that such a universal system poses to citizens’ liberties, the country does not seem alarmed enough. So far, there has been little public debate. A recent study on the public views on DNA database-related matters showed that a more censorious attitude towards wider national databases is correlated with the age and education of the respondents. A deeper public awareness on the benefits and risks of very large DNA collections need to be built and common ethical and privacy standards for the development and governance of DNA databases need to be adopted where the citizen’s perspectives are taken into consideration.

4. Privacy and human rights

Citizens have some worries of privacy and confidentiality issues. The retention of DNA and fingerprints from an individual on a database therefore allows a form of biological tagging or ‘bio-surveillance’, 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 dispute. 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. 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 collection, retention, access and the use of DNA sample that are the basic of DNA profile, 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. People are concerned about potential employers, other government entities or even insurance companies getting access to their genetic information. Insurance companies would have a huge interest in confirming the genetic health of people requesting to be covered by health insurance; employers might also have interest in gaining information about potential employee’s physical health or even ethnicity and ancestry. Access to private information could affect the employability of the person applying for the job.

Concerns about ‘bio surveillance’ extend beyond the state to anyone who can invade the system and obtain access to an individual’s DNA profile. This might include organized 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.

Source of funding

No source of funding.

Conflict of interest

None.

Ethical approval

Not declared.

Acknowledgements

We would like to thank the faculty of the department of Forensic Medicine and Toxicology, King George’s Medical University, Lucknow for their valuable co-operation in this study.

References

2. Environmental Science & Research.
4. Portugal plans a forensic genetic database of its entire population.
7. CODIS – National DNA Index System.
8. Grant Shapps MP Website.
9. Restrictions on use and destruction of fingerprints and samples. National DNA Data Bank*.
18. International Forensic Sciences, DNA Labs India (DLI), Truth Labs and Bio-Axis DNA Research Centre (P) Limited.


