IMPLICATIONS OF DNA IN FORENSIC SCIENCE

Dr. P. Varalakshmi, Associate Professor, Damodaram Sunjivayya National Law University, A.P.

ABSTRACT

DNA technology has shown to be a valuable forensic method in the release of innocent people and the identification of those responsible for violent crimes. These databases are essential in a densely populated country like India. The Union government is working on an updated version of a bill that will establish a central DNA database for "offenders." As is to be anticipated, new problems have emerged as a consequence of the extensive usage of forensic DNA databases. To face the obstacles, numerous methods for growing search capabilities have been suggested, with implementation currently underway. The FBI in the United States has recommended that more autosomal short tandem repeat (STR) loci be applied to its present core range of loci. The endless expansion of forensic DNA databases poses questions about inclusion and retention requirements, as well as concerns about the effectiveness, comparability, and privacy implications of such vast personal data sets. People face problems that extend beyond basic privacy and secrecy concerns. The assay of the disparity or resemblance between two samples is the genetic foundation for forensic DNA study. A, T, G, or C are the basic unit bases of DNA, as is the series of such bases along the DNA strand. Per cell in a person's body has the same DNA. The DNA in a man's blood, for example, is identical to the DNA in his skin cells, fur, sperm, and saliva3. Except for haploid gametes (egg and sperm) and red blood cells, the bulk of cells in the human body are diploid cells with similar DNA (Non-nucleus). Blood, saliva, sperm, skin, feces, and hair, among other biological evidence forms, are widely used in forensic science for DNA analysis. The fact that no two humans had the same genome led to the invention of DNA fingerprinting. “DNA fingerprinting” or “genetic fingerprinting” is a method for identifying patterns in hypervariable regions (HVRs) in DNA. In 1985, Dr. Alec J Jaffrey patented the procedure.

1. INTRODUCTION

"DNA technology has shown to be a valuable forensic instrument in the release of innocent people and the prosecution of serious criminals."[1] Forensic DNA databases aimed to establish investigation leads for investigating crimes, and they were normally under the jurisdiction of "criminal justice departments for law enforcement detection purposes."

In several countries around the world, Forensic DNA databases are now well-established. The United Kingdom developed the first government database (NDNAD) in 1995, preceded by New Zealand. In 1998, France created the Fichier National Automatise des Empreintes Ge ne tiques (FNAEG). The Combined DNA Index System (CODIS) database has been organized by the FBI in the United States. They were originally meant for sex criminals, but have now been expanded to cover nearly every criminal offender.

Anyone convicted on suspicion of a recordable crime in England and Wales is required to request a DNA examination, the profile of which is subsequently recorded in a DNA archive as a permanent report. The DNA profiles of several individuals who are acquitted in Scotland are required by law to be deleted from the database. Just DNA profiles of prisoners that have served more than two years in jail are held in Sweden. Court orders are required in Norway which Germany, and are generally applicable to violent criminals and those convicted of such offenses that are likely to reoffend. But for Idaho, all 49 states in the United States store DNA profiles of criminal criminals, and several even store profiles of victims. In 2005, the newly elected Portuguese government suggested establishing a DNA database for the whole Portuguese community. However, after a lengthy discussion that involved feedback from the Portuguese Ethics Committee, the database launched was restricted to prisoners for the general public.

The United States has the world's biggest DNA archive, with over 9 million documents in the CODIS as of 2011. The National DNA Database (NDNAD) in the United Kingdom is of comparable scale. The scale of this database, as well as its pace of rise, is worrying civil liberties and political parties in the United Kingdom, where police have large powers to take samples and hold them even though they are acquitted. Other countries, such as Qatar, have implemented privately established DNA databases, such as Bode db SEARCH. A variety of

[1] Jeffreys A. Genetic Fingerprinting. Nat. Med. 2005;11:1035–9

datasets contain profiles from missing people and their families, as well as unidentified human remains, in addition to direct matching between recognized and unknown sample profiles.

Missing individual reporting is also a useful tool in the investigation of such offences. A cold hit happens when a match is produced from a national DNA database to connect a crime scene to a suspect who has given a DNA sample to the database. A cold hit is helpful for leading an enforcement force to a potential perpetrator, but it loses the evidential significance of a DNA match produced outside of the DNA database. It has 361,176 forensic profiles and 9,404,747 inmate profiles as of March 2011, rendering it the world's biggest DNA site. CODIS has provided over 138,700 matches to requests as of the same year, helping in over 133,400 inquiries. As of March 2011, the National DNA Database in the United Kingdom included an approximate 5,512,776 human profiles.

As the public's acceptance of DNA databases grows, more states are establishing and expanding their own databases. California actually has the world's third-largest DNA network (naturally, since CODIS incorporates details from all states' databases). California Proposition 69 (2004), which expanded the reach of the DNA database, has also resulted in a substantial rise in the amount of inquiries supported. The use of DNA databases has been broadened to include two contentious areas: arrestees and familial searches. An arrestee is an individual who has been detained but has not yet been convicted of a crime. At the present, 21 states have enacted laws enabling law enforcement to take DNA from an arrestee and insert it into the state's CODIS DNA database to see whether the individual has a criminal background or is connected to any unresolved crimes. The DNA database is used in familial scanning to look for partial matches that can be predicted between near relatives. This technology may be used to connect crimes to perpetrators' family members, assisting in the identification of a criminal even though the perpetrator's DNA sample is not in the database.

As predicted with the great progress of the usage of forensic DNA databases, new threats are emerging. “There is an increased desire for international data sharing, which may be slowed if only a small number of loci is shared; 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 may be slowed if only a small

number of loci is shared."[2]

2. CURRENT SCENARIO IN INDIA

"In a heavily populated country like India, these types of databases are in high demand, since they may assist in the prevention of various types of fraud such as ration card fraud, voter ID card fraud, and driving license fraud, among others."[3] The database could assist Indian police in discriminating between criminals and non-criminals. The Union government is working on a revised version of a bill that will establish a nationwide DNA database of "offenders," calling for the processing and preservation of DNA samples from those convicted of crimes ranging from murder, sexual harassment, and abuse to even breaches of the Motor Vehicle Act.

"The Department of Biotechnology (DoB) formed a committee known as the DNA Profiling Advisory Committee in 2003 to make suggestions for the drafting of the DNA Profiling Bill 2006, which ultimately became the Human DNA Profiling Bill 2007. The Department of the Interior and the Centre for DNA Fingerprinting and Diagnostics collaborated on the 2007 draft Bill (CDFD)."[4] The CDFD is a self-contained organization funded by the DoB. In addition to the CDFD, India has a range of Central Forensic Science Laboratories regulated by the Ministry of Home Affairs and the Central Bureau of Investigation, as well as many private laboratories that analyze DNA samples for criminal purposes.

Activists have criticized the proposed bill as a possible invasion of people's rights and have raised legal and technological concerns about it. Helen Wallace, a member of Gene Watch, a UK-based anti-DNA database organization, believes that India can learn from foreign experiences, especially the United Kingdom, which was the first country to set up a database in 1995, allowing the preservation of DNA records of innocent people. The Protection of Freedoms Act, passed in May, would erase approximately 1 million documents from the archive.

[2] Compulsory DNA Collection: a Fourth Amendment Analysis
Congressional Research Service.
[3] CBS News http://www.cbsnews.com/news/supreme-court-says-police-can-take-dna-swabs-after-arrest/.
[4] Restrictions on use and destruction of fingerprints and samples.
National DNA Data Bank

The UPA government is expected to implement a DNA Profiling Bill in the winter session of Parliament, in a contentious step that promises to expand the state's intrusion into the lives of everyday people. The bill, if passed, would provide the law the power to gather a large volume of confidential DNA data from residents, even if they aren't "suspects" in a criminal case. The information will be kept until the individual has been approved by the court.

“Many privacy activists are concerned by the bill, believing that once it becomes law, it would allow the government to build invasive databases. The bill recommends the establishment of a national DNA data bank, which will be overseen by a joint secretary to the Indian government.”[5] For activists, this would allow the government to take on the part of a terrifying "Big Brother" gathering large amounts of personal information from people. The bill's preamble acknowledges that "DNA analysis provides confidential details that, if misused, can hurt an individual or community." The government has also included a section that requires ‘‘volunteers" to have DNA profiles that would be held on tape. It is unclear under what conditions the "volunteers" would disclose their personal information with the government.

The data can also be used for ‘‘creation and management" of population information, as well as ‘‘identification, analysis, protocol growth, or quality control," according to the law. Surprisingly, the punishment for ‘‘misuse" of DNA profiles is a few months in jail or a paltry Rs 50,000 fine.

In reality, law enforcement authorities such as the CBI (Central Bureau of Investigation) have pressured the government to approve the bill as quickly as possible. They referenced the conclusions of a UK legislative study published in February 2006 by the Office of Science and Technology, which reported that prosecutions in criminal trials rose significantly after the government decided to hold DNA profiling data indefinitely. According to the survey, after DNA samples were loaded into the national DNA database, crime detection in the UK increased from 26% to a safe 40%.

However, since this type of database is often used in conjunction with crime figures, there is concern that minorities may be readily abused. This is an issue expressed in a British legislative survey, which claims that ‘‘blacks and ethnic minorities are poorly portrayed" in their database

[5] Ge J, Yan JW, Budowle B, Chakraborty R, Eisenberg A. Issues on China forensic DNA database. Chin J Forensic Med 2011;26:
252–5.

since they are investigated for suspected offences in greater numbers. At the time, the new bill answers these questions regarding the inherent ethnic disparity in establishing a national DNA database.

"Meanwhile, senior police officials who are acquainted with the bill and have provided detailed presentations to the DBT (Department of Biotechnology) are concerned that the bill contains a clause that allows DNA profile data to be deleted after an individual has been convicted by the courts."[6] They agree that holding the data and eventually growing it can go a long way toward stopping and prosecuting crimes. Although it is a fair point, the lack of a strict privacy law poses questions regarding the current DNA Profiling Bill's invasive existence.

3. BENEFITS AND RISKS

"The endless expansion of forensic DNA databases poses questions about inclusion and retention requirements, as well as concerns about the effectiveness, comparability, and privacy implications of such vast personal data sets. In comparison to the past, DNA research is used to investigate not only major but all offenses, resulting in millions of DNA profiles, many of which are processed and searched in national DNA databases."[7] "When large datasets are collected, new mining procedures based on correlation become possible, as they often do. 'Familial DNA Database Searching,' for example, is focused on close matches between a crime stain and a data-based human, which may be a close relative of the true offender."[8] In 2004, the first familial search was effectively undertaken in the United Kingdom, leading to Craig Harman's manslaughter conviction. Craig Harman of Frimley, Surrey, was found guilty and sentenced to six years in prison after a DNA profile from a nearby relative connected him to the crime scene. The policy has since been implemented in a few US nations, but not at the national level. It was through a dragnet that it was discovered that German police were often engaged in family quest tactics. Police in a small town in northern Germany convicted a young man suspected of rape after examining the DNA of his two brothers who were interested in the dragnet. They had identified the perpetrator based on partial matches between crime scene DNA profiles and these siblings. In comparison to other nations, Germany's Federal

[6] Marjanovic´ et al. Forensic DNA databases in Western Balkan region. Croat Med J 2011;52:235–44.
[7] Combined DNA Index System (CODIS). Available from: http:// www. fbi.gov/about-us/lab/codis/.
[8] ibid

Constitutional Court ruled in December 2012 that potential court usage of this form of testimony will be banned. Alec Jeffreys challenged the way UK police gather DNA profiles early on, maintaining not only violent criminals but even arrestees without indictment, offenders acquitted of an inquiry, and also innocent citizens who have never been charged with a crime. He also stated that broad national datasets, such as England and Wales' NDNAD, are likely to be socioeconomically biased. "The rest of the matches are for small offenses; according to GeneWatch in Germany, 63 percent of the database matches are for robbery, whereas abuse and homicide are for rape and murder."[9] Following a significant setback at the European Court of Human Rights in 2008, the improvements to the UK database were contained in the 2012 Security of Freedoms law. As of May 2013, 1.1 million accounts (out of a total of around 7 million) have been destroyed in order to erase the profiles of innocent users from the database. In 2005, the Portuguese government proposed a DNA database containing samples from all of the country's residents. Given the risks that such a universal structure presents to citizens' freedoms, the nation remains unconcerned. There has been no civic conversation so far. "A new survey of public opinion on DNA database-relevant issues found that a more censorious approach toward larger national databases is related to the respondents' age and schooling. There needs to be a greater public understanding of the advantages and dangers of very broad DNA datasets, as well as general ethical and privacy principles for the creation and governance of DNA databases that take citizens' views into account."[10]

4. PRIVACY AND HUMAN RIGHTS

"Citizens are concerned with questions of anonymity and secrecy. The preservation of an individual's DNA and fingerprints in a database allows for biological marking or "bio-surveillance," and may be used to try and find out where they've been. This ensures that DNA databases may be used to trace people who haven't done something wrong or whose "crime" is a nonviolent demonstration or disagreement. For example, in a state where freedom of expression or civil rights is limited, the police or secret services may try to collect DNA samples from the scene of a political meeting to determine whether such persons have been pre-selected. Searchable digital records with personal demographic details, such as name and nationality, are related to the potential to biologically tag an entity and trace their location using

[9] NPIA UK (Communications), Gav Ireland, Simon Lewis, Dan Fookes (2012–03-31). ''NPIA: Statistics''. Npia.police.uk.
[10] ibid

their DNA profile in DNA databases. Relatives of a person may also be recognized by partial DNA matching. As a consequence, DNA databases change the power dynamic from the person to the state."[11]

These considerations extend not only to the selection, storage, access, and usage of DNA samples, which are the basis of a DNA profile, but also to all other details that might be processed. When DNA is obtained after an arrest and held forever, there is extra material contained in the police archives of the arrest as well as the tests that could be stored in the labs that analyzed them. People are nervous about their genomic knowledge being exchanged with prospective employers, other government departments, or even insurance providers. Care providers might be very interested in confirming the genetic fitness of individuals seeking health insurance, and workers would be interested in learning about future employees' physical well-being, race, and heritage. The applicant's employability can be harmed whether he or she has access to private details.

Concerns over 'biosurveillance' reach outside the government to anybody who can break into the framework to gain access to a person's DNA profile. This may involve organized crime or terrorist organizations, as well as those looking for a specific person. Individuals in victim security programs, for example, may have their appearance changed but not their DNA. When someone becomes suspicious of them and gathers their DNA, their identification may be discovered by comparing it to a stored DNA profile on a website, if one exists and is related to their previous identity. 'Familial hunting' can even contribute to the identification of their kin (looking for partial matches with the DNA profiles of other people on the database). "If the parent has a snapshot of their DNA (taken from an old toothbrush, for example) or shares part of their DNA profile because they are linked to them, children who have been removed from an adult for their safety could be tracked down by those with access to a DNA database."[12]

CONCLUSION

Much like in medical settings, patients require anonymity while DNA data is involved, so in forensic ones, too. Using DNA for reasons other than criminal law or forensic security should be seen as a misuse of the material, which should be prosecuted as such.

[11] ibid
[12] CBS News http://www.cbsnews.com/news/supreme-court-says-po-lice-can-take-dna-swabs-after-arrest/.

It is a popular and understandable practice for prosecution and defense lawyers to understate the scientific importance of DNA evidence. Presentations that claim that DNA testing is perfect are very unlikely and need to be discouraged before making a case in a courtroom.

Methods should be introduced to enable oversight of testing labs and staff.

Some non-forensic organizations conducting regulatory/accreditation of DNA technologies should be independent of corporations, the government, or other labs involved in the work.

Test labs must never be allowed to hide test results from clients on proprietary grounds.

The same scientific principles and procedures employed to examine life science and technological discoveries can also be applied to the application of DNA methods and techniques utilized in forensic science. These efforts should be stepped up to achieve the uniformity of universal norms as well as providing the best available access to science and technological information.