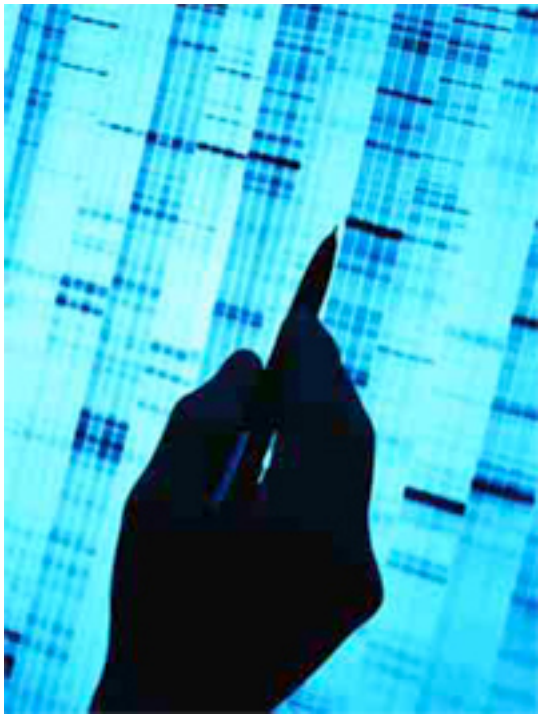
Law Enforcement DNA Databanks Threaten Medical Privacy



In order to prevent and solve crimes, the FBI collects and stores some people's DNA—genetic information that is unique to every individual—in computer databases. In the viewpoint that follows, the Electronic Privacy Information Center (EPIC) maintains that this cataloging of DNA has grave implications for privacy rights. For one thing, the organization claims, DNA information should be protected more than fingerprints are because DNA serves as an identifier and can reveal telling details about people's—and their families'—traits and diseases. Another of EPIC's concerns is that DNA databanks may be breached, resulting in highly sensitive data being released. The group also alleges that the forced collection of criminal suspects' DNA without a search warrant, which occurs in most U.S. jurisdictions, is a privacy violation. EPIC is a public interest research center focused on protecting privacy and other civil liberties.

As you read, consider the following questions:

1. What comprises DNA databanks, as stated by EPIC?

2. In EPIC's opinion, what is worrisome about science's ability to extract more personal information from less material?

3. In discussing the security of DNA databanks, what does EPIC say creates several points at which privacy can be violated?

Genetic information about any organism is contained in the organism's DNA (deoxyribonucleic acid) molecules. DNA is contained in all of the organism's cells except mature red blood cells. Every cell has two pairs of chromosomes, composed of DNA, except gamete cells (sperm and egg), which have only one set. DNA provides exact instructions for the creation and functioning of the organism. DNA molecules of all organisms contain the same basic physical and chemical components, arranged in different sequences. The genome is an organism's complete set of DNA.

DNA and DNA Databanks

The current estimate is that humans have between 32,000 and 35,000 genes. About 99.9 percent of the genome is the same in all humans. The arrangement of the remaining components is unique to most individuals. Only identical twins (or triplets, etc.) have identical DNA. Variations in DNA influence how individuals respond to disease, environmental factors such as bacteria, viruses, toxins, chemicals, and to drugs and other therapies. The interaction between genes and environmental factors is not well understood at this time and is the subject of intensive research.

Any properly stored tissue sample can be the source of DNA. Handbook of Human Tissue Sources, published by RAND, estimated that in 1999 there were more than 307 million tissue specimens stored in the United States, and that the number was growing by 20 million per year. These specimens are collected and stored for research, medical treatment, law enforcement, military identification, blood and tissue banking, fertility treatments and, increasingly, commercial purposes. However, not all tissue collections can be classified as DNA databanks. DNA databanks are composed of a set of tissue specimens, digital DNA profiles, stored in a computer database, and some form of linking between each specimen and the DNA profile derived from it. DNA databanks used in medical and research applications also include links to medical records and family history of individuals whose DNA is stored. Blood and tissue specimens can be preserved indefinitely, and DNA from these specimens can be tested multiple times.

Highly Sensitive Information

Genetic data poses significant privacy issues because it can serve as an identifier and can also convey sensitive personal information about the individual and his or her family. As genetic science develops, genetic information provides a growing amount of information about diseases, traits, and predispositions. At the same time, smaller and smaller tissue samples are required for testing. In some cases tests can be performed with as little as the root of a single hair or saliva left on a glass from which an individual drank. The ability to derive more information from less and less material creates increasing challenges to privacy because it permits analysis of tiny traces that all humans leave behind

unconsciously, such as cells left on computer keys or saliva left on a drinking glass.

The ability of genetic information to provide both identification and sensitive information related to health and other predisposition has led to a lively debate about appropriate privacy protections. Proponents of "genetic exceptionalism" claim that genetic information deserves explicit and stricter protection under the law. They base their argument on the special qualities of genetic material:

* Ubiquity, i.e., the ability to derive genetic profiles from small physical traces and the longevity of material from which genetic profiles can be derived

* Ability to reveal information not just about the individual but also about the individual's family

* Predictive nature that can point to someone's future health and traits

Opponents of "genetic exceptionalism" take the position that genetic information is much like other personal information and should be protected in the same way. They point to the fact that "genetic information" is difficult to define because it includes information like family medical history, which has been collected and used by doctors long before the sequencing of the genome. Therefore, they emphasize the importance of context in which genetic information is obtained and used. For example, if genetic information is obtained as part of health care research or treatment, it should be subject to the same privacy and anti-discrimination protections as all other health information.

At present there is no specific protection for DNA information at the federal level in the United States. ...

The use of DNA in identification is growing. DNA 'fingerprinting' is a process in which a laboratory creates a profile of specific agreed-upon segments ('loci') of the DNA molecule. In order to identify a particular individual, the laboratory compares the profile produced from a sample of unknown DNA with the profile produced from a sample known to belong to an identified individual. The laboratory then calculates a statistical probability that a match could take place purely by chance. The more sections match within the two samples, the higher the probability that the DNA belongs to the same individual. ...

DNA Profiling in Law Enforcement

Law enforcement agencies around the world are increasingly relying on DNA evidence. Although DNA evidence alone can seldom be used to prove that an individual committed a crime, it can be used to place the individual at the crime scene if the scene contains biological evidence. When a DNA profile is derived from evidence at the crime scene, law enforcement officials can search forensic DNA databases for a matching DNA profile to determine whether the evidence came from an individual who committed a prior offence. They can also request DNA samples from suspects or, in some countries, conduct "DNA sweeps" of large numbers of people to find an individual whose DNA matches evidence found at the crime scene. In some cases, when the police have a suspect and know of locations where that individual's tissue samples may be stored, a search warrant may be used to obtain the sample for analysis. The high confidence placed in DNA matches makes it particularly important that biological evidence be handled carefully to avoid contamination and that other evidence be available to link the individual to the crime. DNA evidence has been challenged in courts of several countries because of improper handling during evidence collection or testing.

According to the 2002 global survey by Interpol, 77 of its 179 member countries perform DNA analysis and 41 member countries have forensic DNA databanks, which include both physical samples and databases of DNA profiles. The percentage of members having DNA databanks is predicted to double in the next few years. Interpol is in negotiations to create protocols for searching and sharing DNA profiles across borders as part of its larger initiative on digital communications between law enforcement authorities.

The rules for inclusion in forensic DNA databanks and the rules that govern access to data, physical specimen retention, and privacy protections vary from country to country. In countries that operate under federal systems, such as US and Australia, rules for forensic DNA databanks can vary from jurisdiction to jurisdiction. The United Kingdom has the largest forensic DNA databank, which holds over 2.5 million samples of those who have been charged with one of a list of offenses and, since April 4, 2004, those who have been arrested but not charged.

DNA Databanks in the United States

US law enforcement agencies use databases of DNA profiles, created by the states and linked through the FBI's Combined DNA Index System (CODIS). These profiles contain the analysis of 13 segments of non-coding DNA, i.e., DNA that does not contain information about predispositions or other characteristics, but varies from individual to individual. The CODIS system, authorized by Congress in 1994, allows law enforcement officials to exchange and compare DNA profiles at the local, state and national levels. As of April 2004, over 1.8

million profiles were accessible through CODIS. The samples on which DNA profiles are based, usually blood or saliva, are kept at forensic laboratories around the country. Samples are generally maintained for a long time in order to permit re-testing if DNA profile evidence is challenged or as technology improves.

States in the US have different legislative requirements for inclusion in DNA databanks. All 50 states require sex offenders to provide DNA samples. In addition, some states require DNA samples from some or all felons, and many states include juveniles in their databanks. Samples of convicted offenders, whose profiles are submitted to the CODIS database, are retained indefinitely. State laws vary about the length of time other samples are retained. In at least one case, an individual who had not been convicted is suing the state to demand the return of his DNA sample. Federal and state law enforcement authorities have urged their legislatures to expand the scope of DNA databases. ...

Numerous Privacy Concerns with the Collection, Use, and Storage of Genetic Data

Use of DNA in law-enforcement activities is a subject of debate in the United States and other countries. Civil rights, including privacy rights, are at the heart of the debate.

* Security of DNA databanks: DNA databanks require appropriate safeguards for storage of physical samples, database security for DNA profile databases, and security mechanisms to protect the links between the two. This creates several potential points at which individual privacy can be violated and requires complex and multi-layered security arrangements, as well as appropriate audit and accountability measures. Members of Australian and Scottish law enforcement agencies objected to having DNA of police force members included in DNA databanks in part because they were concerned that security breaches could lead to compromise of police DNA profiles. (Police officers' DNA would be included in forensic databanks in order to eliminate from the investigation biological evidence belonging to officers on the scene. Police officers' fingerprints are routinely included in forensic fingerprint databases for the same reason.)

* Re-use of DNA samples for research, education and planning: Forensic DNA databanks have in some cases been used for research and education. Some have suggested that since tissue samples, which are the source of DNA profiles, contain all the information about individuals' predispositions to disease, they should be used for planning by correctional authorities. Such use of highly personal information without individual consent has been questioned because it is inconsistent with good information practices, which require that personal data be used for purposes for which it was collected or for which explicit informed consent has been obtained from each individual. While an argument can be made that those who have been convicted of a crime lose some of their civil rights, this cannot be said of those who were arrested but never convicted but whose DNA remained in forensic databanks. Although secondary purposes such as research might be accomplished with de-identified information, the Victorian Privacy Commissioner raised doubt that DNA information can ever be permanently de-identified, "given it is essentially comprised of identifiable material." As a result, he proposed that the purposes for which forensic DNA databanks can be used should be clearly defined and subject for public discussion in order to permit appropriate balance between various public policy goals.

* Storage of DNA of individuals who have never been involved in a crime: In some cases DNA has been collected from witnesses or others in order to eliminate them from police inquiries. DNA has also been collected from families of suspects in order to determine whether suspects should continue to be pursued. Since individuals may be reluctant to question the authority of police requesting a DNA sample, it is not clear that individuals can provide truly free informed consent to additional uses of their DNA even when they sign consent forms. If such DNA samples or profiles are included in forensic databanks, the databanks will include many people who have not been arrested or convicted of crimes, and the use of these people's DNA by law enforcement officials and researchers could compromise individual privacy.

* Due process in collection of DNA evidence: Most US jurisdictions do not require consent in order to obtain a DNA sample from someone convicted of a crime. In some countries, police are permitted to use necessary force to collect a sample when a convicted individual refuses to do so voluntarily. It is not clear how many jurisdictions restrict covert collection of DNA samples from suspects, e.g., from a drinking glass or a napkin. Associated Press reported in August 2003 that at least one judge in Iowa ruled that the police did not violate a man's rights when they derived his DNA from a fork and water bottle he had used and left behind. On the other hand, the UK's Human Genetics Commission and the Australian Law Reform Commission recommended that surreptitious collection of DNA be done only if permitted by a search warrant.