

Whose DNA is it Anyway?

Expanding DNA Databanks Raise Human Rights Concerns

Sujatha Byravan

James Watson, one of the discoverers of the structure of DNA, the primary form of inherited genetic material, recently gave permission to a company to sequence his DNA and make the results public. "Provided they didn't release to the world that I have some disease I don't want to know about," he said (From *The Quest for the \$1,000 Human Genome* by Nicholas Wade, *The New York Times*, July 18, 2006).

Watson was right to be concerned about the privacy of his DNA since genomic information can reveal a lot about our inherited tendencies to develop certain diseases. Not only do our genes unveil information regarding our own bodies, but also about those with whom we share our DNA. As scientists learn more about genes in the coming years, additional details are bound to be uncovered. Over the last few decades, there has been a convergence in the expansion of DNA and computer and Internet technologies. As the ability to store, access, and work with large amounts of information has grown, it has catalysed technologies and policies that require or generate even larger sets of data. The complete sequencing of the human genome was regarded as a major challenge and was decoded in 2003 in its entirety. This was heralded as a landmark event, but with faster sequencing speeds using DNA chip technology in which a postage stamp size chip can analyse thousands of DNA markers from a sample, the goals of genomic technology development and the issues appear to have changed quite rapidly. It might soon very well be possible to sequence the DNA of anyone who needs it; perhaps even of everyone in the not too distant future.

Medical and genetic sequence information are increasingly being gathered at a variety of public and private institutions. The UK has proposed a national Biobank with samples from 500,000 volunteers, and the National Institutes of Health in the US has plans for a similar centre. Other institutions that gather DNA samples and store sequence information include hospitals, research institutions, prisons, the military, insurance companies, the police, employers, genetic testing services and counselors. Private companies such as Metropolis (in Mumbai) and Arda's Corporation (in Massachusetts) have gotten into the game and serve as brokers for gathering DNA from people and providing them to third parties.

New computer technologies allow us to collect, store, search and retrieve information as required. Computer technology also allows one to match a specific DNA sequence with a very large data set. If this were not possible, there would be no point in gathering DNA sequence information from a variety of sources as is now being done. It would be cumbersome to work with the sequences and there would be no easy way to use the information efficiently for research. In this paper I discuss some of the concerns that emerge from the combination of DNA typing with computer and Internet technologies. The emphasis being the effects of the merging of these two, I will try to provide an idea of the range of challenges that have emerged and will not necessarily offer a comprehensive analysis of various concerns related to DNA typing.

Let us begin by examining the case of Children's Hospital in Philadelphia (CHOP) to understand some of the problems that could emerge with biomedical research and DNA collection and typing. CHOP announced in 2006 that it would gather DNA from children who came for obesity treatment, raising alarms among a number of observers. The DNA of these children would have been sequenced and the information stored in some conceivably

long-term database. It would then be analysed to identify commonalities shared by this group and require further research to provide clues to the genetic determinants of obesity. The goal was to carry out research so that in future CHOP could test every child who walked in for the presence of the “obesity gene.” If such a gene were ever found, CHOP would patent it and reap profits from anyone using the test. Broad initial consent to use their children’s tissue for research does not cover the range of concerns that parents might have in future. Such concerns might include questions like the following: what additional kinds of research would the DNA be used for; who would have access to the DNA; how can privacy be guaranteed; would employers, insurers and others in the life of the child have access to the information in future and discriminate against them; and what about profits garnered by the hospital using the patients’ tissue. Hospitals such as CHOP have the added ability to combine their medical records with their genetic databases and develop lucrative partnerships with drug companies through their research.

Although law enforcement and the military were previously collecting DNA solely for identification purposes, this situation has now changed. There is clear evidence that in the UK criminal DNA databanks are being accessed for research. In most places, in addition to the DNA sequence itself, the blood or other tissue sample from which the information is obtained is also stored thus making it possible to trace the DNA to a particular person, thus leading to further concerns. This explosion in the gathering and storage of such information is taking place in a number of countries across the world with the UK and the US leading the way. Australia, countries across Europe, Singapore, and Japan are not far behind and there is growing interest and a momentum to the enthusiasm shown by other countries to using DNA typing for a variety of causes from security, personal identity, and immigration to biomedical research and police work.

Concerns About Privacy

The Internet has provided opportunities for the development of an unregulated market in which the consumer can directly buy genetic tests without assistance or interpretation by a doctor or a counsellor. A number of tests with little validity or value are now available over the Internet for anyone eager for such information. Genetic determinism and the idea of “decoding” the future of one’s health is anything but the mere unfolding and expression of ones genes. Despite this scientific knowledge, the popular belief enshrined in the minds of most people is that our genes determine our health futures, our intelligence, behaviour and a range of different characteristics and qualities. Thus many people are quite excited about genetic tests, but there are plenty of reasons to be concerned.

Any collection and storage of DNA information provides opportunities for third parties to access this databank. If the security is breached, we cannot change our DNA at will just as we might change our bank account or credit card numbers. Altering our genetic identity is not possible and therefore we are left vulnerable unable to protect ourselves from the consequences of personal DNA theft. Even in the US, where technologies in this area are quite advanced, there is no legislation that protects an individual’s genetic privacy.

The Council for Responsible Genetics in Cambridge, Massachusetts has gathered evidence of hundreds of instances of discrimination mostly by insurance companies and employers on the basis of a person’s genetic information. One example is the discrimination faced by workers in the Burlington Northern Santa Fe Railroad Company, which the Equal Employment Commission revealed to be conducting genetic tests on its employees without their informed

consent, as a means of counteracting workers compensation claims for job-related stress injuries. In what turned out to be the US government's first case against workplace DNA discrimination, Burlington Northern finally agreed in 2002 to pay \$2.2 million to settle charges.

While there is legislation in some states in the US to protect individuals from discrimination by employers and insurers on the basis of genetic information, this is post-invasion of privacy. Genetic non-discrimination legislation is important, but in the first place no one should have access to a person's DNA information without the person's knowledge and explicit instructions. Just as no one should be able to steal one's credit card details, one's house keys or purse, they should not be able to steal one's genetic information and we need laws that would protect a person's genetic privacy.

Civil Rights

“America has more than two million citizens behind bars, the highest absolute and per capita rate of incarceration in the world. Black Americans, a mere 13 percent of the population, constitute half of this country's prisoners. A tenth of all black men between ages 20 and 35 are in jail or prison; blacks are incarcerated at over eight times the white rate” (From *Jena, O. J. and the Jailing of Black America* by Orlando Patterson, *The New York Times*, Sept. 30, 2007).

Britain's police National DNA database is the largest in the world with the sequence of DNA from a certain region of the chromosome. According to GeneWatch UK, a leading public interest organization, a large number of minorities are in the police database, including 300,000 children and young people between the ages of 10 to 18. Most of Britain's black men (at least 3 out of 4) are in the database. Many countries across Europe are beginning to develop or expand their criminal DNA databanks.

In the US, The Federal Bureau of Investigation (FBI) has a DNA database referred to as CODIS — Combined DNA Index System, which allows local, state and federal officials to enter, store, search and share DNA profiles electronically. In this current post 9-11 climate of fear, conditions for the gathering of DNA from a person have been progressively relaxed. In early 2006, President Bush signed into law the DNA Fingerprint Act, which allows the collection and retention of DNA from individuals who are merely arrested, that is, under suspicion even prior to trial or conviction, or from non-US persons who are detained under federal authorities. This Act also allows states in the US to upload DNA profiles to CODIS. In addition it serves as a green light encouraging states that do not as yet collect DNA from those who are arrested, but are innocent, to move in that direction. It undermines the principle of presumption of innocence. At last count there were seven states in the US that were taking DNA from those just arrested, but there are others considering widening their net in the same manner by changing their policies to gather DNA from arrestees.

Although DNA has allowed many innocent people in prisons to be released, increasing the size of the police DNA database with arrestees does not help in catching criminals. The police try to match DNA found in a crime scene with the DNA in their database and if there is a match, sometimes the perpetrator of the crime is found. Adding an increasing number of innocent people to the police databank does not increase the ability to catch those who perpetrate crimes. On the contrary, it overburdens crime labs and other criminal justice agencies that are ill equipped to handle the large number of samples that they now have to

analyse. The poor, the marginalised, people of colour, other minority groups and people living in certain neighbourhoods and communities are more likely to be regarded with suspicion by the police. Thus when DNA from even innocent suspects is to be included in the database, it is not surprising that the police database is disproportionately composed of DNA from these marginalised groups.

In the US, systematic racial disparities run through every stage of the criminal justice system. They affect who is detained, arrested and convicted, and the kind of punishment that is meted out. About 60 years ago, 22 per cent of the prison population was black and 77 per cent was white, but as of December 2004, according to the Bureau of Justice, 41 per cent were black, 34 per cent white, 19 per cent Hispanic and the rest belonged to 'other' races.

The new DNA technology and storage, easy matches and retrieval through CODIS do not make the system any fairer, but simply varnish the normally biased operations of the police with the patina of legitimacy.

Where are we headed with this new technology of DNA typology? The control of immigration is yet another potential application of this technology. In order to track illegal immigrants, governments could justify collecting the DNA of individuals profiled as 'immigrants' in wide sweeps in the interest of securing the borders. Officials could then keep track of their travel details, and from that, perhaps even glean their tendency for terrorist activities. Since the 1970s, an increasing majority of legal immigrants coming into industrialized nations are from less-developed countries in Asia, the Caribbean, Africa, Eastern Europe, and from Mexico. One could then envision that the DNA of immigrants, who are mostly people of colour and are from poorer countries, would make its way into DNA databases in the West. Further, since scientists are working to identify so-called racial genes, we might be ready to create a racially sub-divided immigrant DNA database. One could also envision law enforcement agencies turning to DNA technology to identify 'home-grown' terrorists, especially since they need no longer have distinguishable 'Middle Eastern' features. For instance, perhaps it may be considered politically expedient to collect the DNA of Arabs or Muslims to make the dominant white constituency in European and North American countries feel safer.

In Conclusion

Technology, not medicine, is the immediate force behind the search for tools that allow for rapid and cheaper genetic sequencing of the human genome. Newer and faster DNA decoding machines are being developed simply because they are possible, not because there is a demand for them. Manufacturers can however be confident that demand will grow as researchers learn more and uncover additional linkages between genes and the occurrence of specific diseases. Even when the push to develop and employ certain technologies is influenced by societal needs, it is also guided by our prejudices and biases. Hand-held devices, not larger than a credit card, that could take a person's DNA and compare it with the information in CODIS were used by the police force on the streets of New York in a pilot programme. This allowed the police to quickly check on individuals who they stopped on city streets. Police DNA databanks in Britain are being accessed by scientists for research into the genetic determinants of criminal behaviour. Even though research has repeatedly shown that there is no genetic link with deviance, some scientists will not cease and the research into this dubious area continues. Many states in the U.S have legislation that permits similar research using criminal DNA databanks. Thus not only will DNA from minorities become a large part of the police DNA database, but their DNA will also be specifically researched to find out

why they have a “tendency” to commit crimes. Then perhaps people could be scanned and those with “criminal genes” could be identified before they carry out crimes, this being the overall goal of such research.

Minority groups such as those who are sick, disabled, people of colour and immigrants, will have their DNA taken by the police more often in different contexts. Thus the confluence of information storage and DNA technologies has fuelled a new sort of Orwellian world in which only certain kinds of people are compromised. The rest will go about their lives feeling secure and just fine. When the problem touches close to home, as it did in the UK when numerous innocent children’s DNA were included in the police database, people who had remained uninvolved or even supported the policies for gathering arrestee DNA joined in the protest. Perhaps this is what it will take to wake people up to the issues involved. We all need to recognize that when the rights and liberties of a few are compromised for the freedom and security of the rest of us, justice is never served. The support and expansion of specific technologies is not value free. In a globalized world, our science, our problems, fears and our technological responses are to a large extent borrowed or transplanted and what is done in one place is extended and applied to other parts of the world. Therefore, DNA typing will spread to various countries; in what form and how fast depends on a number of contextual factors.

What kinds of limits can be placed on DNA databanks? There should be legislation that ensures privacy and protects from discrimination on the basis of genetic information. Limits on police databanks such as including only the DNA of convicted felons and not providing open access to researchers is important. Getting rid of samples once the information is entered is another safeguard. As new genetic technologies are sought to keep the world safe, it will require an acute vigilance to be sure that while we attempt to create a safe place for some people, we do not end up with new social order that results discrimination and apartheid for others.

References

1. Roche PA, Annas GJ. (2001) Protecting genetic privacy. *Nat Rev Genet* 2:392-396.
2. Patricia A. Roche, J.D., and George J. Annas, J.D., M.P.H. (2006) DNA Testing, Banking, and Genetic Privacy. *NEJM*, Volume 355, No. 6: 545-546
3. <http://www.gene-watch.org/>
4. S, Byravan (2006) DNA Typing: A technology of fear *Development* 49, 28–32.
5. Paul R Billings (2005) Genetic nondiscrimination *Nature Genetics* 37, 559 – 560.
6. Duster, Troy (2003) *Backdoor to Eugenics*, second edition. New York: Routledge.
7. Duster, Troy (2004) 'Selective Arrests, a DNA Forensic Database, and Phrenology', in David Lazer (ed.) *DNA and the Criminal Justice System; The technology of justice*, Cambridge, Massachusetts: MIT Press.
8. Gosline, Anna (April 9–15, 2005) 'Will DNA Profiling Fuel Prejudice?', *New Scientist* 186(2494): 12.
9. Hacker, Andrew (2003) *Two Nations: Black and white, separate, hostile, unequal*, New York: Scribner.
10. Lewontin, Richard (2005) 'The Fallacy of Racial Medicine', *Gene Watch* 18(4).