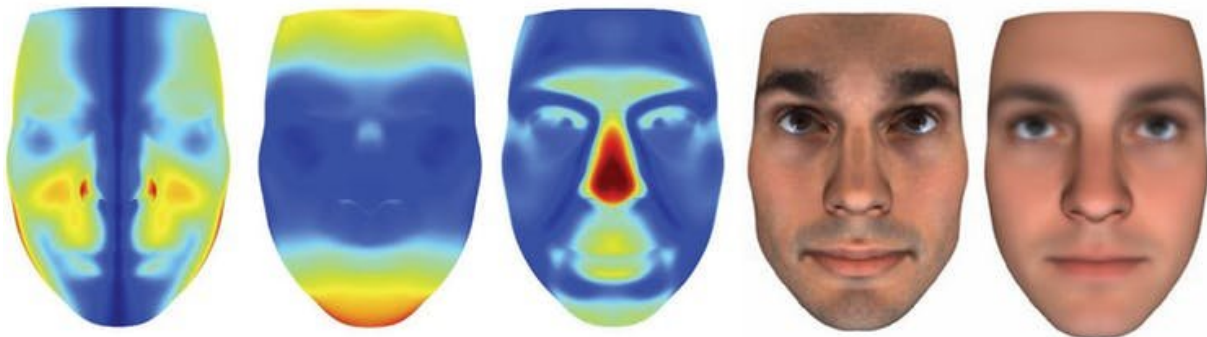# Dramatic advances in forensics expose the need for genetic data legislation

December 19 2018, by Caitlin Curtis, James Hereward, John Devereux, Karen Hussey And Marie Mangelsdorf

We're getting better at predicting physical traits, like faces, from DNA data. Credit: Composite from PNAS

Many people first became familiar with DNA testing through its use in the OJ Simpson murder trial in 1994. Now, 24 years later, there have been two dramatic advances in the capability of forensic genetics that mark the start of a new era.

The first is the amount of information we can predict about a person from DNA found at a crime scene, and the second is the way police can use open genealogy databases to identify people.

But we need to be careful how we use these new tools. If people lose

trust in how DNA data is used and shared by police, it could have an adverse impact on other applications – such as medical care.

That's why we're calling for a [Genetic Data Protection Act](#) to ensure people have confidence in the way their DNA is accessed and used.

We can learn a lot more from DNA now

[Predicting traits from DNA](#), known as "DNA phenotyping," is improving. Facial prediction, health traits, predisposition to disease, even personality traits and things about our mental health can be predicted from genetic data. Some [researchers](#) are even considering predicting propensity to drink or smoke.

Law enforcement agencies around the [world](#) are using these traits to create predictive DNA "mugshots," but in many countries there is no specific regulation on how and when they should be incorporated into policing.

And some types of predictions raise considerable ethical issues.

For example, should it be OK for [law enforcement](#) to predict the mental health or disease risk of a suspect? If so, should that information be used in a trial? If law enforcement predicts a high risk of a particular disease, should they be compelled to tell a suspect or their family?

Separation between databases is breaking down

You may be familiar with "CODIS" from CSI, this is the database that law enforcement has traditionally used to identify DNA collected at a crime scene. CODIS has around [17.7 million](#) DNA profiles. There are strict rules around who can be included in these databases, and the vast

majority of profiles are from convicted offenders.

According to best estimates, the number of people who have taken genetic ancestry tests is slightly higher than this, and police have started using this data as well. The type of data in CODIS only allows close family matches, but the type of data in open ancestry databases allows much deeper relations to be found.

Even if you haven't participated in genetic testing or made your genetic data public, you may have a relative who has. Currently, law enforcement is able to identify people based on matches as distant as third cousins.

On average, people have around 190 third cousins. One estimate indicates that over 90% of Americans of European descent already have a third cousin or higher in the open genealogy database GEDmatch. It may take as little as 2% of the population uploading their DNA data in a genealogy database for the entire population to be identified this way.

New statistical methods mean separations between previously distinct genetic databases are disappearing. Traditional forensic markers can now be cross referenced to ancestry data, even though they are completely different types of genetic data. This means close family members could be identified across different databases. These methods can also be used to re-identify subjects in medical genetics research projects.

There has been a lot of public support for the use of genetic genealogy to catch serial killers and rapists. In some cases, people are voluntarily uploading their data to help these efforts.

The 238 relatives in your generation that might be affected if you share your genetic data. Credit: image designed by James Hereward and Caitlin Curtis

But where should we draw the line? Should genetic data only be used in

serious crimes, or are we happy to have a comprehensive system of genetic surveillance that covers the entire population?

Private companies are aiding law enforcement

Both [DNA phenotyping](#) and forensic genealogy – which relies on amateur genealogists – are now being offered to law enforcement by [private companies](#).

Parabon, a US-based pharmaceutical company, has partnered with armchair genealogist [Cece Moore](#). She started using genetic genealogy to find the parents of adoptees and children born through sperm donation, but now uses it to catch criminals.

Parabon also offers facial prediction services. While the science of facial prediction from DNA is getting better, it is still contentious, and several prominent scientists have cast [doubt](#) on whether Parabon can really do what it is promising.

Nevertheless, this move out of government labs and into private ones raises questions about oversight – and what exactly is happening to the data generated.

Genetic data is different from other kinds of data

Genetic data is highly unique and can be thought of as a personal 15 million letter pin-code. Since the code doesn't just identify us, it also contains important information about our disease risk, personality traits and even our physical features like our face, it is very difficult to keep anonymous.

Unlike a [credit card](#) we can't request a new genome if our data is

compromised. And a stolen credit card won't tell a perpetrator anything about the finances of our family members.

We understand what happens if we lose a credit card, but our understanding of genetic data is still developing. And we're likely to see it put to unexpected uses in the future.

We need a "Genetic Data Protection Act'

Technological advances in genomics are outpacing public awareness, and existing legislation doesn't fit genetic data well. Under current laws, the lab that produces the genetic data has ownership of the record. But if our genetic data represents a deep part of the essence of us, it shouldn't be this easy for us to give up ownership of it.

We need new ways to protect genetic data to maintain trust in medical genomics. Sometimes people need their genome sequenced for medical purposes, but they might be reluctant to consent if trust has broken down around how genetic data could be used. That could result in poorer medical outcomes.

One solution to prevent this is a specific "Genetic Data Protection Act," which would grant people ownership of their own data. However, it must be different from standard property rights: ownership should be immutable and nontransferable.

The issues around use of our genetic data are complex, individuals (and their descendants) must be protected. Under no circumstances should it be possible for an individual to unwittingly sign an agreement that results in a loss of control of their genetic data. Legislation is part of the solution, but education and new technological solutions will also be important.

The recent introduction of the digital [My Health Record](#) shows that Australians care about who is accessing their sensitive information. And people are already [expressing unease](#) about the confidentiality of their genetic data.

We must establish clear boundaries about how genetic data generated for medical purposes is used – whether by police or by any other interested parties. Giving genetic data the protection it needs, and making sure that medical [genetic data](#) doesn't become a forensic resource will be crucial to ensure public trust in medical genetics.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation