Is your genome really your own? The public and forensic value of DNA

May 2 2018, by Nathan Scudder And Dennis Mcnevin

Women who remain unidentified at the time of burial are named Jane Doe. Credit: Findagrave

When Joseph DeAngelo was arrested in the United States last month over a series of 30-year-old murders and assaults, attention quickly focused on how the suspect was found.

In their search for the so-called "Golden State Killer", police looked for DNA matches on a public genealogy database that people use to build family trees. This approach led police first to a close relative, and then to the suspect.

Applying genealogical research techniques to forensic DNA analysis is a useful tool in solving cold cases.

However – as many who have traced their family tree would know – genealogy is not for the fainthearted. It is a complex and difficult process, prone to error and misinterpretation. Family trees have been described as "entangled meshes".

Without expert knowledge, false assumptions can be made and investigative resources wasted. The technique also raises legal, ethical and policy challenges.

Identifying human remains

In 1981, a woman wearing a buckskin jacket was found murdered on a roadside in Ohio. The unidentified "Buckskin Girl" was buried in a "Jane Doe" grave. While investigators pursued various leads, DNA obtained from retained blood yielded no matches.

In 2018, the DNA Doe Project – a new charity applying a technique called "forensic genealogy" to unsolved missing person cases – agreed to work on the case.

Using crowdfunding, the volunteers collected donations to undertake

"whole genome" sequencing. This generated enough genetic data, consistent with the markers used by online DNA providers, to allow upload to a public genealogy site.

The search returned a possible first cousin, once removed. By searching that individual's shared family tree, a presumptive identification was made. The family tree included a comment about a relative: "Death—Unknown Missing—Presumed Dead".

In a matter of hours, genealogists had provided a solid lead in a 37-year-old case, leading to the identification of the victim as Marcia King.

There are about 500 sets of unidentified human remains in Australia. Given the success of genealogists at the DNA Doe Project, applying this approach could help bring closure to families.

Where things can go wrong

Law enforcement use of forensic genealogical data has not always yielded such results.

In 1996, Angie Dodge was murdered in Idaho. DNA was recovered from the crime scene and, nearly 20 years later, the profile was searched against a genealogy database. A close match was returned and investigators identified that individual's son, Michael Usry Jr., as a suspect.

However, Usry, who was coincidentally on vacation in Idaho around the time of the murder, later provided a DNA sample and was ruled out as the culprit. Usry says that it took a month to clear his name through DNA.

Search engines still return results linking him to the investigation. While

almost all hits make clear that he was eliminated as a suspect, one asks: "Do you think Michael Usry Jr. could be involved in Angie's murder?"

Will people be put off genetic testing?

The potential for online genetic databases to be used to help law enforcement is increasing – the DNA testing market is expected to more than triple by 2022, to A$388 million. In 2017, AncestryDNA – the largest provider – reportedly sold 1.5 million test kits in a single sales weekend alone.

But use of forensic genealogy also has the potential to undermine consumer trust in genetic testing and online genealogy.

Genetic providers may be more susceptible to consumer backlash about privacy concerns than social media companies such as Facebook, which has continued to grow in spite of recent concerns about its data storage practices. Many users do not find the need to engage with genetic providers on an ongoing basis, like they do with Facebook. After initial testing, users wishing to minimise privacy risks could potentially download their data and then delete their accounts, preventing the company from further using their data.

Genetic providers are also limited in their ability to implement privacy safeguards, such as identity verification, due to the very nature of their products. Individuals may legitimately use the tool without knowing their true birth name or names of family members.

In each of these cases, investigators uploaded of some form of genetic data, of unknown origin, to a public database. This could amount to a breach of a provider's terms and conditions, but there may be little the company can do to prevent such use.

We should proceed with caution

Forensic genealogy is just one example of the growing intelligence value of publicly accessible data. Police have also used social media to track suspects. A coroner in Idaho noted that: "Facebook is not something we thought we'd be using to find next of kin. We use it every single week."

This kind of law enforcement activity online has been litigated in the past.

In a 2014 US case, evidence was admitted despite police obtaining access to a social media account by inviting the defendant to accept a fake friend request. Here the defendant explicitly consented, but genealogical websites often promote the sharing of family tree and genetic information, without requiring consent to share with each new connection.

This followed a 2013 example where the US Drug Enforcement Administration allegedly created a fake social media account in the name of the owner of a seized mobile phone. In that case, the social media provider wrote demanding no other fake accounts be created on its platform.

Similar arguments may arise with forensic genealogy. Courts may need to balance the benefits to society of solving crime with whether the user has given implied consent, both for themselves and their relatives.

Privacy legislation may also kick in at the point where a profile is identified, or is reasonably identifiable. When that occurs, the forensic genealogist has created an online genetic profile for a third party, without their consent.

The use of forensic genealogy brings us closer to a point where it may be

possible – given enough data and resources – to identify any genetic sample. Crowdsourcing and crowdfunding means this technique is available to all.

Achieving an approach that is privacy compliant, balanced and cautious is essential to maintaining public trust and minimising potential harm. Otherwise individuals who, having parted with $99 and a small vial of saliva, may suddenly find themselves part of a criminal investigation.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation