COMMENT | Genetics inMedicine

Open

Protecting trust in medical genetics in the new era of forensics

Caitlin Curtis, PhD[1,2], James Hereward, PhD[2], Marie Mangelsdorf, PhD[1], Karen Hussey, PhD[1] and John Devereux, DPhil[3]

Genetics in Medicine (2019) 21:1483–1485; https://doi.org/10.1038/s41436-018-0396-7

We have recently witnessed two dramatic advances in the capabilities of forensic genetics. First, the use of public genealogy databases to identify criminals (as publicized by the Golden State Killer case), and secondly, the advancing science of trait prediction in forensic investigations. Just as the 1995 OJ Simpson murder trial brought the existence of DNA forensics (and some of its shortcomings) into the public consciousness,[1] in our opinion, these two developments, 23 years later, mark the start of a new era in forensic genetics.

These nascent capabilities raise issues of privacy and consent that extend well beyond forensics. Significant public concern has already been reported surrounding access and use of genetic data,[2] but the discourse around the introduction of genetic genealogy and phenotyping approaches has been limited, disjointed, and unfocused. As forensic genetics and medical genetics converge toward genome sequencing, issues surrounding genetic data become increasingly intertwined—and cannot be viewed in isolation. What happens to our genetic data in one realm, such as forensics, is highly likely to affect how society trusts the use of genetic data in medicine. The speed of these developments has surprised many and demands a policy response to protect trust in medical genetics.

POLICE GENEALOGY

Since the high-profile arrest of the alleged Golden State Killer, police around the world are digging through their freezers looking for samples.[3] One company has launched a "Genetic Genealogy" service to commercialize the technique. The first 100 samples run through their system reportedly yielded 20 strong matches, several of whom have already been arrested.[4]

Traditionally, forensic databases used around 20 markers, which only allowed direct matches or close family relationships to be inferred. In the Golden State Killer case, police took DNA from a crime scene and generated the same kind of data as consumer ancestry companies. These companies use "SNP chips" that read around 700,000 markers and are dramatically more powerful for making genealogical inferences. Police then created a profile and searched the data against GEDmatch, a publicly accessible genealogy database of genetic information shared by people pursuing an interest in genealogy, including searching for long-lost relatives.

Police did not match close relatives but made a number of third and fourth cousin matches. We have around 190 third cousins in an average family.[5] Our genetic connections to these distant relatives mean that the actions of people we have never met have put many of us within reach of this new law enforcement tool. One approximation suggests over 90% of the American population with European ancestry already has a third cousin in GEDmatch, which has around a million users. Accessing the data on a larger system, such as AncestryDNA (~10 million users), puts that estimate at 98%[6].

GEDmatch users (prior to the adjusted terms and conditions) did not specifically and knowingly consent to the use of their genealogy data by law enforcement. Even if individuals do consent to this use, their family members might not. Consent given by one person should not bind others.

Genomic databases already have a diversity problem.[7] Police genealogy will likely exacerbate existing biases by increasing fear and distrust of genetics in minority groups. Police genealogy also goes to the heart of the broader issue of surveillance, and the extent to which we are prepared to sacrifice our privacy to enforce the law.

PREDICTIVE FORENSIC GENETICS

Ethical and legal frameworks around forensic genetics are heavily influenced by the "noncoding" nature of the current markers, which have little connection to physical traits (except sex determination). Forensics is in the process of a

[1]Centre for Policy Futures, The University of Queensland, Brisbane, QLD 4072, Australia; [2]School of Biological Sciences, The University of Queensland, Brisbane, QLD 4072, Australia; [3]TC Beirne School of Law, The University of Queensland, Brisbane, QLD 4072, Australia. Correspondence: Caitlin Curtis (c.curtis@uq.edu.au) or James Hereward (j.hereward@uq.edu.au)

Submitted 31 July 2018; accepted: 26 November 2018
Published online: 18 December 2018

dramatic shift from these "noncoding" DNA fingerprinting methods, to tests that tell us much more about a suspect.

Several companies are offering "DNA phenotyping" services. Parabon Nanolabs (Virginia) predicts skin, eye, and hair color, freckles, ancestry, and face shape, producing a DNA "mugshot". DNA phenotyping has been used in the Netherlands, France, the United Kingdom, Canada, Australia, and several US states, although in many countries there is little legislation regulating its use (but see[8]).

Outsourcing forensic services to private companies such as Parabon raises questions about governance and oversight. The generation of sensitive genetic data, especially by nongovernmental agencies, also raises questions about security, use, and access. Are warrants required to access it? Is the data destroyed if a suspect is found not guilty? Is deletion even feasible given data retention requirements of laboratory certification? Transnational transfer of genetic data outside its original jurisdiction can also result in a loss of legal protection, although there are some protections for the international transfer of personal information (i.e., restrictions in the Privacy Act in Australia, and under the General Data Protection Regulations [GDPR] in Europe).

The science behind predicting physical features from DNA is advancing rapidly, but the ability of current approaches has been hotly debated in the scientific community[9] (also see Erlich unpublished preprint https://www.biorxiv.org/content/early/2017/09/07/185330.1). The methods and algorithms that underpin commercial phenotyping services have not been published and have largely escaped scientific scrutiny. How can we trust the accuracy of the algorithms when no one has the ability to view the code or verify the results?

Predicting physical features from genetic data works better for some ethnicities than others. For example, traits like eye and hair color are relatively invariant in Korean populations, making current phenotyping tools less useful. Researchers in that country are considering predictive tests for other, nonphysical traits such as propensity to drink, or likelihood to smoke.[10] This raises the ethical question of where the line is drawn, and what traits we allow to be predicted.[11] Predisposition to diabetes, Marfan syndrome, obesity, schizophrenia, bipolar disorder, and personality traits, among others, have been suggested as potential phenotypes that could be implemented in the future (despite ethical concerns).[12]

Making medical or behavioral predictions raises issues of disclosure and prejudice that have received little attention. If law enforcement finds that a suspect has a high risk of a disease are they obliged to tell them, or should they respect the "right not to know"? Would law enforcement need expertise in genetic counseling, or would this require a liaison between law and health services? Currently these methods are mostly used to generate leads, and not presented as evidence in court. If this kind of information was disclosed, however, then how might it affect jurors in a trial? Could it even be used in support of the defense or prosecution's case? If so, what level of confidence would be required given that genetic inferences are generally probabilistic rather than deterministic?

THE NEED FOR GENETIC DATA PROTECTION

These developments illustrate two major issues. Police genealogy shows how one person's decision about their genetic data can impact not only close relatives, but distant ones. DNA phenotyping highlights how much sensitive information is contained in our genetic data.

Some jurisdictions have made provisions allowing the use of health information by law enforcement in circumstances deemed to be reasonable. Genomics alliances around the world are generating genomic information from millions of individuals. Genetic information generated in a health setting must be protected, and not become a forensic resource, to ensure public confidence in medical genomics.

Attempts have been made to limit genetic discrimination by some jurisdictions, but the developments outlined here suggest that policy should focus on the thing we need to protect—genetic data.

The creation of a Genetic Data Protection Act would provide governance on the broad issues of access, storage, and use of genetic data. Our view is that genetic data *is* different from other data. It contains highly sensitive information that is *unique* to us. If our genetic data is compromised we cannot request a new genome. Genetic data is very difficult or impossible to anonymize, particularly as our ability to predict physical traits becomes more refined. What happens to our genetic data affects not only us, but our relatives, and consequences extend to subsequent generations. Genetic data needs more protection than other types of data. Individual ownership of digital genetic data is a fundamental right that a Genetic Data Protection Act should grant.

Ownership of genetic data needs to be different from standard property rights. It should be immutable and nontransferrable. The issues around use of our genetic data are complex, and vulnerable individuals (and their descendants) must be protected. It must not be possible for an individual to unwittingly sign an agreement that results in loss of control of their genetic data. These rights must also be provided in a way that preserves existing protections against the patenting of human genes. Genetic data is often spread across many jurisdictions, so protection would preferably be granted internationally. Ideally this would be through international treaty, but other mechanisms for extraterritorial protections have recently been demonstrated with the creation of the European GDPR.

As the technology for not only reading, but also editing DNA improves, the issue of ownership is only going to become more important. The law is already failing to catch up to advances in genetic technology. In establishing protection for genetic data, future technological advances and potential uses or misuses must be considered.

Discussions about the use of genetic data have been happening for almost two decades, and limited protections have been granted, in some jurisdictions (e.g., the Genetic

Information Nondiscrimination Act in the United States). In some instances, excellent proposals have been made, but not implemented.[13] Several international declarations have been made by UNESCO on the governance of human genetic data, but these guidelines need to be translated into local law for genetic data to be fully protected. The new era of forensic genetics exposes the inadequacy of current legislation and should be the catalyst for granting full and proper protection to our most personal information.

DISCLOSURE

C.C. receives financial support from the University of Queensland and the Queensland Genomics Health Alliance. J.H. receives financial support from the University of Queensland, the Australian Cotton Research and Development Corporation, and the Australian Government Department of Agriculture and Water Resources. M.M. receives financial support from the University of Queensland and the Queensland Genomics Health Alliance. K.H. receives financial support from the University of Queensland and the Queensland Genomics Health Alliance. J.D. receives financial support from the University of Queensland and the Queensland Genomics Health Alliance.

REFERENCES

1. Butler JM. Fundamentals of forensic DNA typing. Amsterdam: Academic Press/Elsevier; 2010.
2. Associated Press–NORC Center for Public Affairs Research. The June 2018 AP-NORC center poll [GENE10]. July 2018. https://reports.norc.org/issue_brief/genetic-testing-ancestry-interest-but-privacy-concerns/.
3. Maron DF. Cold cases heat up as law enforcement uses genetics to solve past crimes. Scientific American. 2 July 2018. https://www.scientificamerican.com/article/cold-cases-heat-up-as-law-enforcement-uses-genetics-to-solve-past-crimes/.
4. CISION PR Newswire. Parabon announces Snapshot genetic genealogy service for law enforcement. 8 May 2018. https://www.prnewswire.com/news-releases/parabon-announces-snapshot-genetic-genealogy-service-for-law-enforcement-300644394.html.
5. Henn M, Hon L, Macpherson JM, Eriksson N, Saxonov S, Pe'er I, Mountain JL. Cryptic distant relatives are common in both isolated and cosmopolitan genetic samples. PLoS One. 2012;7:e34267.
6. Edge MD, Coop G. How lucky was the genetic investigation in the Golden State Killer case? The Coop Lab. 7 May 2018. https://gcbias.org/2018/05/07/how-lucky-was-the-genetic-investigation-in-the-golden-state-killer-case/.
7. Popejoy AB, Fullerton SM. Genomics is failing on diversity. Nature. 2016;538:161–164.
8. Vogel G. German law allows use of DNA to predict suspects' looks. Science. 2018;360:841–842.
9. Lippert C, Sabatini R, Maher MC, et al. Identification of individuals by trait prediction using whole-genome sequencing data. PNAS. 2017;114:10166–10171.
10. Seo HJ, Cho S, Lee JH, Lyoo SH, Kim MY, Lee SD. Forensic DNA phenotyping: a review in Korean perspective. Korean J Leg Med. 2017;41:23–31.
11. Scudder N, McNevin D, Kelty SF, Walsh SJ, Robertson J. Forensic DNA phenotyping: developing a model privacy impact assessment. Forensic Sci Int Genet. 2018;34:222–230.
12. Silva de Cerqueira CC, Ramallo V, Hünemeier T, et al. Predicting physical features and diseases by DNA analysis: current advances and future challenges. J Forensic Res. 2016;7:1000336.
13. Australian Law Reform Commission and Australian Health Ethics Committee of the National Health and Medical Research Council. Essentially yours: the protection of human genetic information in Australia (ALRC 96). 2003. https://www.alrc.gov.au/publications/report-96.