Privacy Law
Bulletin

Privacy and the search for suspects using forensic genetic genealogy

Nathan Scudder *UNIVERSITY OF TECHNOLOGY SYDNEY*

Introduction

New DNA technology, when combined with online commercial genealogy databases, is now providing investigative leads to law enforcement. Balancing privacy will be important as more recreational DNA testing makes it likely that anyone leaving genetic material at a crime scene will also leave clues as to their distant relatives.

Key points/ how does it affect you?

- Forensic technology can now predict certain physical characteristics or the biogeographical ancestry of the donor of a trace of forensic relevance and, by comparing with online genealogy data, provide investigators with information about their potential relatives.
- Privacy legislation predominantly focuses on the personal and sensitive information of people who are identified or reasonably identifiable. The DNA of a person, such as a suspect, deposited at a crime scene does not, at the time analysis is undertaken, fit into that category.
- The broader issue of privacy interests of family members has now given rise to discussion about "genetic informants" — individuals whose DNA has helped catch distant criminal relatives.
- Increased use of new technology will require careful balancing of society's interests in catching offenders with individual privacy interests, as well as consideration of how best to allocate scarce investigative resources.

Overlaying data in search of criminals

In 2010, Wendy Kramer, the founder of the Donor Sibling Registry stated that: "With DNA testing and Google, there's no such thing as anonymity anymore".[1] Her teenage son had, 5 years earlier, sent away his own genetic sample to a commercial genealogy company. After identifying a common ancestor with two other genetic contributors to the database, he became one of the first — and almost certainly the youngest at the time — to identify their sperm-donor father using genetic genealogy.[2] This technique has since been described as "[l]ike Facebook, but for fifth cousins".[3]

The use of DNA in prosecuting a defendant for a crime is based on "assigning a biological origin to [genetic material from a crime scene] with a high degree of statistical certainty".[4] Such an approach relies on a direct comparison between a crime scene sample and a sample obtained from a suspect or convicted offender, generally by taking and analysing a buccal swab from that person.

New DNA technology presents many opportunities to provide investigators with leads in cold cases where traditional investigative processes have not identified a suspect. Advances in genetic technology have allowed forensic laboratories to invest in DNA sequencing capabilities which can cost-effectively analyse crime scene traces and allow scientists to make predictions about a suspect's physical appearance or biogeographical ancestry.[5] These capabilities adapt biomedical applications for use by forensic investigators.[6] In doing so, they raise similar privacy considerations to other investigative leads based on open source information, but also give rise to ethical considerations around the use of sensitive information in the form of genetic data.[7]

From the early days of recreational genetic genealogy, it was arguably inevitable that the technique would collide with forensic science to form a new investigative tool — *forensic genetic genealogy* — the ability to search for suspects by finding relatives, close or distant, in online public genealogy databases.[8] The efficacy of these new capabilities increases as datasets grow. It has been predicted that only 2% of a population group need to be included in a database to present a high level of confidence of finding at least one third cousin or closer relative, when searching a sample of unknown origin from within that population group.[9]

This does not mean that forensic genetic genealogy will work all the time. In addition to available public genetic data, there is a need for a considerable amount of genealogical and investigative research to identify a suspect. The most prominent use of forensic genetic genealogy was to identify the Golden State Killer in

California in 2018. This case reportedly involved 8000 investigative hours researching family trees back to 1800s, before ultimately narrowing the search to a single suspect.[10]

Privacy and public databases

As technology changes so can the privacy lens through which we view the potential for that new technology to deliver benefit to society.[11] Commentators have written about the rise of "Big Data policing" in recent years, but the underlying principle has not changed since the detective and their notebook.[12] The tools at the disposal of an investigator have dramatically increased information-gathering and analysis capabilities. These new capabilities can help find suspects and solve crimes but — almost invariably — there is a trade-off with privacy.

The concept of "privacy-invading technologies" and the growing push for "privacy by design" in information system is not new.[13] Commentators have urged caution as new genomic capabilities invite "scope creep" in police use of DNA.[14] Implementing an appropriate framework around the use of new genomic capabilities can help mitigate both legal and ethical risks upfront, delivering operational outcomes while implementing appropriate checks and balances.[15]

Another key aspect is the changing public conversation around DNA, and the potential for this to lead to increased public expectation that police will use available tools, with due care and diligence, to apprehend a suspect who may otherwise go free.[16] A survey in the United States has already shown nearly four in five of respondents supported use of the technique for violent crime or crimes against children, but less than two in five supported its use for non-violent crime.[17]

A company in the United States established its own genetic database for people to voluntarily upload their genetic sequence, exclusively for law enforcement to find any distant, criminal relatives or to solve unidentified human remains cases.[18]

Privacy in discarded DNA

The Privacy Act 1988 (Cth) establishes key definitions around personal information and sensitive information. Similar concepts are incorporated in state and territory privacy laws. Expanded use of crime scene DNA to identify suspects relies on exceptions. Firstly, at the time analysis or data matching is being conducted, DNA from a crime scene is not associated with an individual. As it is not reasonably identifiable, many of privacy safeguards in the Privacy Act do not apply.[19] This approach to de-identified information is not unintended: it underpins broader genetic and medical research.

At the point when investigators form a hypothesis as to identity, either by using forensic genetic genealogy or through other leads, it is necessary to rely on exemptions for enforcement-related activities: at the federal level, Australian Privacy Principle (APP) 6.2.[20]

A family donation: "genetic informants"

The Australian Law Reform Commission noted in 2003 that genetic information has "a familial dimension" and the Commission did explore, in relation to the health sector, the potential for a record to contain information about two or more people.[21] However, while affording genetic information a high degree of protection, Australian privacy laws offer no ability to disentangle the shared nature of genetic information.

Whether relatives of an offender, such as the Golden State Killer, should be afforded specific privacy protections has been a matter of debate. Relatives whose DNA has been used to catch an offender have even being referred to as "genetic informants".[22]

In many ways, this categorisation is not entirely inaccurate, in that the use of forensic genetic genealogy provides investigative leads in the same way as any other tip-off. However, while identification of those relatives occurs on a public database, investigators only see the proportion of DNA shared between each user on that database and their suspect. This enables investigators to predict the nature of that relationship: the more shared DNA, the closer the relationship is likely to be.[23]

At that point, investigators need to access other personal information about the relatives identified. This would include searching births, deaths and marriages records to identify that individual's parents, grandparents and even perhaps their great-grandparents. In order to search these records, where not publicly available, investigators would again need to rely on the exception for enforcement-related activities in APP 6.2. Once investigators reach back to records about family members who are deceased (and to the extent those records do not also include information about living descendants, or are protected by extension of state or territory privacy laws to recently deceased), the APPs would cease to apply.[24]

Protection from harm and the "right not to know"

The "right not to know" is generally discussed in the context of diagnostic medicine, particularly hereditary disease.[25] But similar ethical difficulties do arise in genetic genealogy. Until now, the capability has largely been confined to hobbyist and some professional genealogists, many of whom would fall outside the scope of privacy laws in Australia. But genealogists recognise

that genetic profiles of the dead can speak to sensitive information of the living. Genetic genealogy may identify illegitimate children or cases of misattributed parentage which may cause distress to individuals and families.[26]

In one sense, individuals are unlikely to discover family secrets through the new tool of forensic genetic genealogy. Police build family trees for one purpose: to create a list of one or more individuals who, based on their family relatedness, may be their suspect.[27] In theory, these family trees should never see the light of day. Once a suspect is identified, existing forensic procedures legislation could allow police to request, or in some cases compel, that individual to provide a DNA sample. This new sample can then be compared directly to the original crime scene evidence.

Once a matter proceeds to prosecution, privacy laws generally yield to the jurisdiction of the courts and the overriding public interest in justice. In addition to obligations on the prosecution around disclosure, a defendant could, if they can establish a legitimate forensic purpose, subpoena details of the genealogy process that ultimately led to their arrest. Even for sensitive information, such as genetic data, there remains a strong public interest in disclosure,[28] more so for genealogy records.

Accordingly, consideration of balancing the interests of privacy must occur earlier in the process, as a fundamental component of the framework around delivery of new DNA technology. A privacy-compliant and ethical use of this data throughout the investigative process can help maintain public trust and confidence.

Conclusion

Developments in genomic technology, and the increase in publicly available genetic data, presents opportunities for investigators to find suspects and to return unidentified human remains to their families. It is timely to consider whether, with these new tools, are we now at a point where — if enough investigative time and effort is applied — almost any suspect can be identified from their discarded DNA.

Forensic genetic genealogy is already a technique which will never hit a dead-end. If no relatives are found the first time, police need only wait for more users to upload data. But, once one or more presumptive relatives are found, finding the suspect can be quite time-consuming. Its use requires careful consideration of the allocation of scarce police (and expert) resources.

Its reliance on privacy exceptions for enforcement-related activities is part of a broader balance between solving crime and minimising privacy implications for third parties. However, embedding considerations of privacy and proportionality throughout the lifecycle of this technique can help safeguard public trust and confidence, while also bringing closure to victims and their families.

Acknowledgments

The author would like to thank his doctoral supervisors at the University of Canberra, with whom he has previously published research. This article builds on this earlier research in an Australian privacy context. The author would also like to thank Mr Malcolm Crompton for his valuable feedback on the manuscript.

Nathan Scudder
Industry Fellow
University of Technology Sydney
Nathan.Scudder@uts.edu.au
www.uts.edu.au

Footnotes

1. R Lehmann-Haupt "Are Sperm Donors Really Anonymous Anymore?", *Slate* 28 February 2010, https://slate.com/human-interest/2010/02/dna-testing-makes-it-easy-to-find-the-identity-of-anonymous-sperm-donors.html.
2. M Angrist "Genetic privacy needs a more nuanced approach" (2013) 494(7435) *Nature*, www.nature.com/news/genetic-privacy-needs-a-more-nuanced-approach-1.12363; W Kramer "Sperm donors who wish to remain anonymous just shouldn't donate" *Huffpost* 28 July 2015, www.huffingtonpost.com/wendy-kramer/sperm-donors-who-wish-to-_b_7878688.html.
3. A Krueger, "Are Genetic Testing Sites the New Social Networks?" *The New York Times* 16 June 2018, www.nytimes.com/2018/06/16/style/23-and-me-ancestry-dna.html.
4. P Claes, H Hill and M D Shriver "Toward DNA-based facial composites: preliminary results and validation", (2014) 13 *Forensic Science International: Genetics* 208–216.
5. C Børsting and N Morling "Next generation sequencing and its applications in forensic genetics", (2015) 18 *Forensic Science International: Genetics* 78–89.
6. F Stajano, et al "Forensic genomics: kin privacy, driftnets and other open questions", in *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, 2008 pp 15–22.
7. A G Ferguson, *The Rise of Big Data Policing*, New York University Press, New York USA, 2017.
8. N Scudder, et al, "Policy and regulatory implications of the new frontier of forensic genomics: direct-to-consumer genetic data and genealogy records", (2019) 31(2) *Current Issues in Criminal Justice* 194–216.
9. Y Erlich, et al, "Identity inference of genomic data using long-range familial searches" (2018) 362 (6415) 690–694.
10. T Arango "The Cold Case That Inspired the 'Golden State Killer' Detective to Try Genealogy" *The New York Times*,

3 May 2018; P Kneeland "East Area Rapist — Long Term Cold Case Investigation" Phoenix, Arizona, 26 Sep 2018.

11. C Farivar, *Habeas Data: Privacy Vs. the Rise of Surveillance Tech*, Melville House, Brooklyn NY, 2018; M Wienroth, "Governing anticipatory technology practices. Forensic DNA phenotyping and the forensic genetics community in Europe", (2018) 37(2) *New Genetics and Society* 137–152.
12. Farivar, above and above n 7.
13. A Cavoukian "Privacy by design: The 7 foundational principles", (2009) 5 *Information and Privacy Commissioner of Ontario, Canada*; D Klitou "Privacy by Design: addressing the escalating technological threats to privacy and civil liberties" (2015) 12(1&2) *Privacy Law Bulletin* 12.
14. J Gans "DNA identification, privacy and the irrelevance of Australian law" (2007) 3(9) *Privacy Law Bulletin* 110.
15. KG Claw, et al "A framework for enhancing ethical genomic research with Indigenous communities" (2018) 9(1) *Nature communications* 2957; N Scudder, et al "A law enforcement intelligence framework for use in predictive DNA phenotyping" (2019) 51(1) *Australian Journal of Forensic Sciences* S255–S258.
16. Farivar, above n 11.
17. CJ Guerrini, et al, "Should police have access to genetic genealogy databases? Capturing the Golden State Killer and other criminals using a controversial new forensic technique" (2018) 16(10) *PLoS biology* e2006906.
18. Othram Inc, DNA Solves, 2019 available at https://dnasolves.com/.
19. M Smith and GF Urbas "Regulating new forms of forensic DNA profiling under Australian legislation: familial matching and DNA phenotyping" (2012) 4(1) *Australian Journal of Forensic Sciences* 63–81.
20. Above n 8.
21. Australian Law Reform Commission *Essentially Yours — The Protection of Human Genetic Information in Australia,* Report 96 (2003) vols 1 and 2.
22. E Haimes "Social and ethical issues in the use of familial searching in forensic investigations: insights from family and kinship studies" (2006) 34(2) *The Journal of Law, Medicine & Ethics* 263–276; T R Brown "Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers" (2019) 21 *Colum Sci & Tech L Rev* 1.
23. E M Greytak, C Moore and S L Armentrout "Genetic genealogy for cold case and active investigations" (2019) 299 *Forensic Science International* 103–113.
24. Office of the Australian Information Commissioner. *What is personal information?* 5 May 2017 available at www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.
25. Brown, above n 22; R Chadwick, M Levitt and D Shickle, *The right to know and the right not to know: genetic privacy and responsibility*, Cambridge University Press, Cambridge, 2014.
26. S Zhang "When a DNA Test Shatters Your Identity" *The Atlantic* 17 July 2018.
27. Scudder, above n 8.
28. W Keough "Human Genetic Information, Genetic Registers and the Subpoena Duces Tecum: Balancing Privacy, Confidentiality and the Administration of Justice" (2004) 16 *Bond L Rev* i.