Privacy Implications of the new ‘omic’ technologies in Law Enforcement

Paul Roffey 1, Nathan Scudder 1,2

1 Australian Federal Police, PO Box 401, Canberra, Australian Capital Territory
2 University of Technology Sydney, Sydney, New South Wales, Australia,

Corresponding author: Paul.Roffey@afp.gov.au

Abstract
‘Omic’ technologies have opened a new revolution in law enforcement and are now solving decades-old cold cases as well as current investigations. The Golden State Killer case is probably the most notable of the cold case investigations that has been solved by one of the new ‘omic’ technologies, namely forensic genetic genealogy. The resolution of this case epitomises the power of the ‘omic’ technologies to solve crime whilst simultaneously unearthing serious legal and ethical concerns around the individuals’ privacy in the use of their genetic information. The legislation that is currently used by the state, territory and Commonwealth jurisdictions in Australia to regulate the use of DNA for criminal investigation is now two decades old and does not address the application of ‘omic’ technologies to criminal investigation. The Australian government is reviewing current privacy laws, and this review could include the use of ‘omic’ technologies. In the absence of specific legislation, law enforcement must continue to develop processes to consider privacy, law and ethics around the use of ‘omic’ technologies for criminal investigation and the identification of human remains.

1. INTRODUCTION
It has been nearly forty years since DNA profiling was used for the first time to solve serious crime. In 1983 and again in 1986 two young girls from two different towns in Leicestershire in England went missing and were later found murdered. Both had been raped and strangled. Police believed the crimes were linked and had arrested a suspect who had admitted to the crimes. Police approached Professor Alec Jeffreys from the University of Leicester to assist with the investigation of the double rape-murder. In the years preceding, Professor Jeffreys had identified repetitive DNA sequences in human DNA that could distinguish individuals and ascertain relationships between family members. When applied to the samples from the murders and the suspect, Professor Jeffreys confirmed the
semen samples from the victims were from the same person but these were not a match to the man they had in custody. Shortly following, a large scale manhunt was launched to find the man who matched the DNA profile. Over the next few months over 5000 men from the local area were screened but no match was found. Six months later a woman reported overhearing a conversation where a local man claimed to have given blood on behalf of a colleague, a man by the name of Colin Pitchfork. Pitchfork was apprehended and his blood taken and confirmed as a match to the DNA profile from the victims (Wambaugh, 1995).

The Leicestershire murders introduced DNA profiling as a forensic science. In the years since, DNA profiling technologies based on the analysis of repetitive sequences have been refined, extended and enhanced and have been complemented by the use of databases for the storage and comparison of DNA profiles generated from crime samples, suspects and convicted offenders. Importantly, laws have been developed to provide the legal framework for the storage and use of DNA profiles and the collection of samples from persons of interest for comparative purposes. In Australia, these laws were based on the Model Forensic Procedures Bill (Parliament of Australia, 2000) which was endorsed by the Standing Committee of Attorneys-General in 1994. Over the period from the late 1990s to early 2000s, the Commonwealth and State and Territory jurisdictions in Australia passed laws based on this model, so that a legal framework was available for the comparison of DNA profiles within and between State, Territory and Commonwealth jurisdictions.

Law enforcement in Australia is now entering a new era of forensic DNA analysis where ‘omic’ technologies will open new avenues for investigation by mining genetic information from forensic samples. This perspectives paper explores the privacy implications that may be generated when the new ‘omic’ technologies are applied to law enforcement.

2. ‘OMICs’ - A NEW HORIZON FOR LAW ENFORCEMENT

DNA profiling has revolutionised forensic science in the latter stages of the twentieth century and has been a powerful tool for law enforcement since. Indeed, it has become the gold standard for forensic identification methodologies. Yet, as powerful as DNA profiling may be, the new and emerging ‘omic’ technologies are ready to extend forensic identification methodologies to a whole new level of identification where ‘omics’ will frequently be used to predict physical traits such as eye, skin and hair colour, hair structure, age and ancestry, predisposition to hair loss and freckling, stature and body
mass index, fingerprint characteristics and facial metrics, and personal details such as surname and consanguinity (i.e. blood relations) (e.g. Kayser, 2015; Shah et al., 2015; Ho et al., 2016; Kling & Tillmar, 2019; Kukla-Bartoszek, et al., 2019.). Although yet to become routine forensic tests, these predictive ‘omics’ are already proving extremely useful for law enforcement having recently solved a number of cold cases (Katsanis, 2020). Importantly, these new and emerging technologies have the potential to take this much further, predicting behavioural and medical predispositions, mental health and cognitive disorders, predisposition to substance abuse and active substance abuse, active medical ailments and current therapeutic treatments (Lawrie et al., 2019). The opportunities made available to law enforcement by the application of ‘omics’ means the level of private information that is reasonable to access for a law enforcement purpose will need to be carefully considered and defined.

Imagine a Police intelligence report for an unidentified person of interest that contains personal details that were predicted from the biological material collected from an exhibit:

“A male DNA profile, referred to as Male 1, was obtained from the handle of the knife relating to XXXX. The Male 1 profile has been placed onto the DNA database for matching purposes. The nucleic acid from the knife was analysed using predictive omics. Male 1 is almost certainly a Caucasian male, 25-35 years of age, 165-180 cm tall, lean build, blue eyes and brown hair. Surname and consanguinity testing have identified a known offender that matches this description, Mr John DOE (DOB XXX). Predicted fingerprint patterns correlate with those on record for John DOE (FP Record XXX). Officers are advised that Male 1 demonstrates a strong genetic predisposition for irrational behaviour and/or violence. Forensic Intelligence assesses Male 1 is almost certainly John DOE (DOB XXX). John DOE has a criminal history for residential burglaries and possession of methamphetamine and drug-related paraphernalia.”

Although still on the boundary of reality, this is not science fiction. At the current rate of discovery this should be possible sometime within the next two decades. Recent history leaves little doubt that there will be public pressure for law enforcement to adopt this technology as it becomes available. It is reasonable to assume the nature of the information these new ‘omic’ technologies will produce for law enforcement purposes will have the potential to impact on the privacy of individuals.

**What are ‘Omics’**
‘Omic’ is a term that is used to describe the fields of science that are used to study the function of biological systems. It is used as a suffix to form words that describe the examination of a biological system in totality. For example, genomics is a field of science (and associated technologies) that examines the structure, function, evolution and inheritance of genomes. Epigenomics studies the reversible chemical modifications to the DNA and DNA-associated proteins in a cell that modify gene expression. Transcriptomics surveys the expression of genes using the total RNA transcription product whereas proteomics explores the overall level of protein composition, structure, and activity. There are many more ‘omic’ disciplines including glycomics, lipidomics, metabolomics, metagenomics, phenomics, cytomics and so forth.

2. ‘OMICS’ AND PRIVACY – PAST, PRESENT AND FUTURE

Privacy is a concept that influences all aspects of our life but at its core it is profoundly difficult to describe because it differs between individuals, genders, social groups, age groups, socio-economic background, cultures, countries, and so forth. The Office of the Australian Information Commissioner defines privacy as “a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination” (OAIC, 2020). Privacy is a fundamental right for all individuals. This right has been acknowledged in several international treaties and conventions (OHCHR, 2020).

Privacy represents many different ideas, including physical privacy, private communications, freedom from undue surveillance, having control over one’s own personal information, freedom from discrimination and the rule of law. The balance between privacy and public security is a constant struggle for members of law enforcement, security and defence agencies, who, on a daily basis, are required to balance the rights of the individual against those of the public within the legal framework at the time.

The authors argue that privacy should be the driving force behind the governance of the ‘omic’ technologies when applied to law enforcement. When looking for guidance on how to meet privacy requirements, forensic science normally turns to the medical fields to see how to implement new technologies within a framework of privacy. However, while medical sciences have made some advances in this area they are still currently imbedded in significant debate around the ethical, legal and social implications involved with the use of ‘omic’ technologies (e.g. Demkow & Wolańczyk, 2017;
Interestingly, the privacy aspect is not necessarily the dominant topic in this debate, rather the primary focus is around how to apply risk prediction equally to all members of society (e.g., Lévesque et al., 2018; Taylor & Barcelona de Mendoza, 2018). Although there are aspects of overlap between medical application and forensic science, there is nothing currently in medical science that could be readily adopted in forensic science use.

In developing these principles, forensic science needs to consider what makes 'omic' technologies different from current and previous forensic biological identification methodologies. The authors would argue the difference is that 'omic' technologies can access personal information about the individual that was not previously accessible to forensic scientists. But, is this true?

Prior to the DNA revolution forensic scientists used blood groups and polymorphic proteins to distinguish and identify individuals. We now know the ABO, rhesus (Rh), Lewis (Le) and Duffy (Fy) blood groups are associated with an array of medical predispositions (Anstee, 2010). Similarly, the polymorphic proteins phosphoglucomutase-1 and haptoglobin have been linked to a variety of congenital disorders, inflammatory diseases and susceptibility to infectious disease (Morava, 2014; Vanuytsel et al., 2013). Early DNA typing systems which used HLADQA1, various Polymarker loci and ApoB had variants that have been associated with various medical predispositions; examples include chronic obstructive pulmonary disease, malaria, celiac disease and coronary heart disease (Megiorni & Pizzuti, 2012; Martinelli et al., 2010; Young et al., 2010; Bigham et al., 2018; Friedl et al., 1990).

Current DNA profiling loci can also reveal sensitive personal information. For example, genetic syndromes that are caused by chromosome aneuploidies are revealed by modern DNA profiling loci; Downs syndrome by D21S11 and Penta D, Edwards syndrome by D18S51, Patau syndrome by D13S317, and Turners and Klinefelters syndromes by the amelogenin locus. The amelogenin locus can also reveal persons inflicted with amelogenesis imperfecta, a disorder that affects the enamel on teeth. Variants at vWA and TPOX are associated with venous thromboembolism (Meraz-Rios et al., 2014), D8S1179, D5S818 and D2S1338 with gastric cancer, and TH01, D18S51 and D2S1338 with psychiatric disorders (Wyner et al., 2020). Any of the genomic markers that are used for forensic identification (i.e. STRs, SNPs, interspersed repeat sequences) can reveal persons who have mosaics, either natural or artificial.
In the same manner, non-genomic-based biological tests reveal sensitive personal medical information. Microscopic examination of blood can reveal leukemias and thalassemias (Bunyaratvej et al., 1985; Scotti, 2005; Mohapatra et al., 2013; Harms et al., 1986) and the presence of active infections (Weitzman, 1975). Microscopic hair analysis reveals information about the donor’s health status (Chu et al., 2020). Microscopic analysis of semen stains can reveal information on the donor’s fertility and whether the donor has been vasectomised (Bartoov et al., 1982; Hancock & McLaughlin, 2002). The microscopic flora present on oral and vaginal swabs can reveal medical conditions such as thrush and bacterial infections (Paladine & Desai, 2018; Marty et al., 2015).

Other biometric disciplines can also be brought into this argument. For example, there is evidence that digit length ratios, and fingerprint and palm print patterns are statistically associated with some human congenital conditions (Eichler et al., 2018, Sai Sankar et al., 2018). Similarly, facial metrics can identify inherited genetic disorders such as Downs syndrome (Zhao et al., 2014; Starbuck, et al., 2011), Noonan syndrome and Velo-Cardio-Facial syndrome (Hammond et al., 2004). Shoeprints may reveal stance and gait abnormalities (Badiye et al., 2020) and bitemarks can show dental characteristics. Teeth can reveal age and dental history (Shah et al., 2019).

So, if personal information has been available to forensic scientists for decades, then why are the authors advocating the importance of overlaying privacy principles on the use of ‘omic’ technologies? The authors argue that the potential for intrusion of forensic analyses on privacy has never been as significant as it is now. Where previous forensic analyses could only reveal personal information as a by-product of the specific information being sought, the ‘omic’ technologies produce personal and sensitive information as a matter of course. In addition, our understanding of how DNA impacts privacy has evolved. When legislation was introduced to regulate the use of DNA profiling and DNA databases in Australia, the significance of the genetic information revealed by DNA profiling was not fully understood. Indeed, when introducing the Crimes Amendment (Forensic Procedures) Act to the Australian Parliament in 2001, Commonwealth Attorney-General, the Hon Daryl Williams made the following statement in his Second Reading Speech (ALRC, 2003):

“It is important that we all appreciate the nature of the forensic information that will be stored on the national law enforcement database as a DNA profile. The analysis of the DNA samples will only reveal the sex of the person from whom it is taken. It does not reveal any other personal characteristics.”
Around the same time, a separate bill was put forward to the Australian Parliament to develop a regulatory framework specifically for genetic information. The bill, called the Genetic Privacy and Non-discrimination Bill, introduced by Democrats Senator Natasha Stott Despoja in 1988, did not pass Parliament (Australian Government, 1998). This suggests the impact of the genetic technologies upon privacy was not fully realised at the time. Indeed, at the time these bills were presented to Parliament DNA profiling was not considered to be significantly intrusive from a privacy perspective because the procedure only analysed loci in the non-coding regions of DNA, which at the time was often referred to as “junk DNA.” We now know there is little DNA in the human genome that has no function. Indeed, from a functional perspective the definition of what constitutes a “coding” region of DNA is ambiguous given the complex regulatory interactions between non-coding and coding regions of the genome. This is reflected by the fact that 37.5% of the HlrIsPlex SNP loci that are used for eye and hair colour prediction and over 90% of the Kidd SNP loci that are used for biogeographical ancestry prediction are within non-coding regions of DNA (Walsh et al., 2013; Kidd et al., 2014).

The authors argue that the difference between previous DNA based technologies and the ‘omics’ is the extent of the personal information that is collected. There is no doubt that forensic genomic methodologies will evolve from the technologies that are being used now, that limit the collection of sequence data to specific target loci, such as those provided by the ForenSeq™ DNA Signature Prep kit (Verogen) and Precision ID Ancestry Panel (Thermofisher, to technologies that will allow the collection of sequences for whole genomes which may also include epigenomic and transcriptomic information. Whole genome sequence generation provides the data that can be used for any genome based analysis. This is incredibly appealing from a law enforcement perspective because one data set can be used for identity through traditional STR or SNP markers, genealogy, biogeographical ancestry prediction, prediction of hair, eye and skin colour, facial metrics, fingerprint pattern prediction, and so forth. However, it also offers opportunities for misuse should analysis move beyond law enforcement investigative requirements such as revealing predispositions to heritable medical or behavioural disorders.

The other aspect that should be considered is that the genetic information that is owned by the individual is also owned by the individual’s relatives so any intrusion on the privacy of the individual is also an intrusion on the privacy of the individual’s family members. The ability of genetic genealogy to establish relationships between distant relatives highlights that the need to establish the rights of
privacy for family members has never been more pertinent. Although this was considered in detail in a report submitted to the Australian Government Attorney-General’s Department in 2003 (ALRC, 2003) the familial nature of genetics has never been fully reconciled with privacy.

There is also the cultural aspect to consider. For example, in the Māori culture, genes and genomes are related to “ira” and “whakapapa”. Ira represent a spiritual inheritance as well as a biological or physical inheritance and whakapapa describes the connections between people and their responsibilities to past, present and future generations. The storage and use of human biological material is therefore a culturally significant issue [Aotearoa New Zealand Law Commission, 2020]. In Australia it has been several years since the last Federal Parliamentary or ARLC enquiry into the forensic use of DNA (Part 1D review). There is very little in these reviews dealing with cultural issues around DNA for indigenous populations in Australia and nothing akin to the work that has been done in New Zealand in the context of new ‘omic’ technologies.

The Commonwealth Attorney-General’s Department is currently conducting a review of the Privacy Act 1988 to determine whether the scope and enforcement mechanisms remain fit for purpose (Australian Government, 2020). Submissions to the review closed in November 2020. Interestingly, very few of the submissions put forward any familial considerations associated with the privacy of genetic information and those that did related this need from a clinical perspective. A discussion paper outlining possible options for reform is expected to be released by the Attorney-General’s Department in 2021. It will be interesting to see whether the ownership of genetic information from a familial perspective is discussed and whether the law enforcement aspects will be considered.

The time is right for users of ‘omics’ in the criminal justice system to enhance their formal processes and to consider broader ethics of business practices, potentially through the establishment of an institution-wide ethics committee.

Ethics committees are common in institutions that conduct human health related activities. Typically, ethics committee have three primary functions; 1) as an educator for the application of ethics within the institution; 2) provide assistance with the development and implementation of policies and workflows to minimise privacy intrusion, and 3) conduct retrospective reviews of the application of ethics on investigations to reflect upon the issues encountered and make recommendations for required policy changes (Annas & Grodin, 2016). A fourth function that would be useful to the application of ‘omics’ in criminal justice would be to act as a consulting authority for active cases that
require changes in the application of privacy principles over the course of an investigation. An ethics committee will not solve all the issues associated with the impact of law enforcement on privacy but would be a good “check point” to ensure privacy is considered.

A recent review conducted by the New Zealand Law Commission recommended the implementation of an independent committee for the oversight of forensic or police DNA testing and DNA databases [Aotearoa New Zealand Law Commission, 2020]. One of the key functions of the “DNA Oversight Committee” would be to monitor developments in the operation of DNA legislation and to advise forensic providers or police when change is required to ensure their practices remains properly aligned to its purpose. A second key function of the “DNA Oversight Committee” would be to assess any proposals from the forensic provider or police to add or remove analysis techniques and advise the Minister regarding these proposals. Such a committee is an extension of the idea, proposed earlier, of institution-wide ethics committees.

**Conclusion**

There is little doubt that ‘omic’ technologies will revolutionise law enforcement investigation through the provision of leads generated by the prediction of physical and behavioural traits from the genetic information left behind at crime scenes. It could be argued, at its core, genetic-based prediction does not represent a fundamental change in criminal investigation. After all, current investigative techniques use eye witness accounts, CCTV footage and so forth, to generate physical and behavioural composites for persons of interest. With-that-said, the authors argue the fundamental difference is the process not the product. ‘Omic’ technologies can generate vast amounts of genetic information, only a portion of which is used to generate the products that are used by law enforcement. The genetic data in totality presents the greatest risk to privacy because it has the greatest potential for unforeseen consequences. Without question, the genetic data extracted from ‘omic’ technologies contains information not yet known, that in the future could be accessed for purposes that are outside of, or on the fringe of, the remit of law enforcement, such as health prediction or the abuse of ancestry inference.

The words of Mr Spock in *Star Trek II: The Wrath of Khan* (1982) could equally apply to considering privacy when implementing ‘omic’ technologies into law enforcement:

> Do “The needs of the many outweigh the needs of few, or the one”?"
Funding Information
Nil to declare

Research Resources
Nil to declare

Acknowledgments
Nil to declare

Notes
Nil

References


Research and Public Health, 15(10), 2072. https://doi.org/10.3390/ijerph15102072


https://doi.org/10.1002/ajmg.a.20665


https://doi.org/10.1136/jcp.55.11.812


https://doi.org/10.1016/j.jid.2015.10.062


https://doi.org/10.1146/annurev-genom-111819-084213


https://doi.org/10.1016/j.fsigen.2015.02.003


https://doi.org/10.1016/j.fsigen.2014.01.002


https://doi.org/10.1016/j.fsigen.2019.06.019


Morava, E. (2014). Galactose supplementation in phosphoglucomutase-1 deficiency; review and

https://doi.org/10.1016/j.ymgme.2014.06.002


https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx


https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0001/01bd081#:~:text=In%201994%2C%20MCCOC%20produced%20a%20draft%20Model%20Forensic


Taylor, J. Y., & Barcelona de Mendoza, V. (2017). Improving -Oomics-Based Research and Precision


**Further Reading**

Nil recommended.