DEVON TESORIERO

POLICE SEARCHES OF CONSUMER GENEALOGICAL SERVICES: AN INVESTIGATIVE GOLDMINE OR A SIGNIFICANT PRIVACY CONCERN?

Submitted for the LLB (Honours) Degree

Faculty of Law

Victoria University of Wellington

2020

Abstract

DNA technology is fundamental in police investigations. The benefits of this technology have resulted in a tendency in New Zealand, and across the world, to expand what DNA is available to police. This paper explores what would be a significant expansion of the DNA the police currently have at their disposal: consumer genealogical services. These services hold millions of DNA samples which are sent voluntarily from individuals looking to explore their ancestry. The fact that these services hold genetic data gives them the potential to be an invaluable asset to police. However, despite the apparent investigative benefits of these services, they also raise significant privacy concerns. This paper has argued that despite societal benefits of crime prevention and public safety, unregulated use of these services will unduly interfere with privacy rights. This paper has analysed the existing law in New Zealand and found that police searches of consumer genealogical services would be unlikely to breach either the Privacy Act 1993, or the New Zealand Bill of Rights Act 1990. Therefore, if the New Zealand Police were to search these services, there would be limited recourse against their actions the privacy intrusion. Consequently, this paper has argued that reform is needed which would permit police to search these services in a restricted set of circumstances, while also upholding the privacy interests of those who submit their DNA.

Key words: *Consumer genealogical services; genetic data; police investigations; R v Alsford; New Zealand Bill of Rights Act 1990; Privacy Act 1993.*

Contents

I Introduction

Since the mid-1980's, DNA (Deoxyribonucleic acid) technology has revolutionised police investigations. A DNA profile can be obtained from a biological sample found at a crime scene, and then compared to samples of known persons in the DNA databank.[1] If the samples match, then it is likely they came from the same person.[2] Unsurprisingly, this technology is a vital resource for police, as it allows them to find or eliminate suspects for investigative purposes.

In 1995, New Zealand enacted the Criminal Investigations (Bodily Samples) Act (CIBS) to facilitate the use of DNA in police investigations.[3] Initially a restrictive approach was taken to DNA profiling, however reforms to the CIBS Act over the years illustrate the tendency in New Zealand for the DNA databank to expand, allowing greater numbers of samples to be analysed and compared.[4]

But this is just the tip of the DNA iceberg, as police now have the potential to access millions of genetic samples without any oversight or regulation. Consumer genealogical services (CGS) allow consumers to submit a biological sample for the purpose of exploring their family tree, ethnicity, or even their families health[5]. One site, Ancestry.com, boasts having over 15 million people in their database, as well as "billions of historical records and millions of family trees".[6]

It did not take long for police overseas to take advantage of this vast amount of biological information. In the United States of America (US) police were initially able to surreptitiously upload a crime scene sample to the service GEDmatch.[7] However, once this technique became

---

[1] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* (NZLC IP43, 2018) at 15.
[2] At [1.6].
[3] At [4.4].
[4] Criminal Investigations (Bodily Samples) Amendment Act 2003; Criminal Investigations (Bodily Samples) Amendment Act 2009. See also Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [75-79].
[5] Ancestry.com "Ancestry - Home" <www.ancestry.com>.
[6] Ancestry.com "About Us - Overview" <www.ancestry.com>.
[7] Jocelyn Kaiser "We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans" (11 October 2018) Science <www.sciencemag.org>

publicised, many of these sites responded by preventing undercover searches, and police could no longer secretly upload information without permission from the service.[8]

In the US, Federal Rules require police to identify themselves before undertaking such a search.[9] New Zealand currently has no regulation of police access to CGS, however they have been discussed by the Law Commission in their report *DNA in Criminal Investigations*.[10] Other than this report there has been minimal discussion about the use of this technology in the New Zealand context.

This paper intends to fill that gap by undertaking a detailed analysis of CGS, the potential benefits, and the privacy risks of permitting police to search them. Chapter II begins by providing an overview of genetics and genetic groups, which will provide context for the subsequent chapters.

Chapters III and IV examine the opposing viewpoints; on one hand, advocates argue that this technology is an investigative gold mine, and limitations on police searches will unduly impede police activities. On the other hand, allowing police to search CGS has raised serious privacy concerns that proponents of this technology often overlook.

After considering the privacy implications, Chapter V analyses whether police searches of CGS would be subject to any safeguards under the existing law. From this discussion it will be clear that reform is necessary to ensure privacy interests are adequately protected.

Underlying any reform will always be various policy objectives. These will be outlined in Chapter VI, before reform options are finally introduced in Chapter VII.

---

[8] See GEDmatch.com "Terms of Service and Privacy Policy" (20 May 2018) <www.gedmatch.com>.
[9] The United States Department of Justice "Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes" (press release, 24 September 2019).
[10] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 190.

Overall, this paper will show that while CGS do have potential benefits, this comes at the cost of unreasonable genetic surveillance which threatens civil liberties. Therefore, reform must be adopted to minimise unwanted state intrusion into genetic privacy.

II Genetics and Genetic Groups: An Overview

DNA is a chemical found in nearly every cell in the human body.[11] A genome is an organism's complete set DNA, which is unique for each individual.[12] Because the genome is unique, it is "completely inalienable", and therefore a biological sample can be used to identify an individual.[13] Accordingly, genetic data is, by nature, deeply revealing.

Not only is DNA revealing in the sense that it can reveal "the most intimate details" about an individual, but it can also reveal genetic groups.[14] Human reproduction involves copying genetic information, which is then passed down between generations.[15] Therefore, there is significant overlap in the genetic make-up between members of the same family. Consequently, one person's DNA can be used to "extrapolate information about family members", who can then be classified into a genetic group.[16]

III Police use of Consumer Genealogical Services: Supporting Arguments

The success of this technology in overseas jurisdictions has prompted advocates to highlight the societal benefits of CGS, including crime prevention, public safety, and efficiency. The following chapter acknowledges that giving police access to CGS would be advantageous for police investigations, however this will ultimately need to be balanced against the less tangible, but nonetheless fundamental, right to privacy.

---

[11] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 6.
[12] At 7.
[13] Dara Hallinan and Paul de Hert "Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law" in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017) 175 at 178.
[14] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [37].
[15] Hallinan and de Hert, above n 13, at 178.
[16] At 179.

A Crime Prevention: an Investigative Gold Mine

Proponents of police use of CGS suggest an attractive argument; that modern technology should be utilised to apprehend potentially violent offenders. Arguably, the societal benefits of solving crimes outweighs the imposition on privacy rights. This is not a new idea, in *R (LS and Marper) v Chief Constable of South Yorkshire Police,* Lord Steyn recognised that it is of "paramount importance that the law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science."[17] This is undoubtedly an attractive premise, particularly when dealing with violent crimes.

Proponents may also point to the recent successes of this technology. In 2018, investigators were able to apprehend Joseph DeAngelo, the alleged "Golden State Killer", after nearly four decades.[18] DeAngelo was suspected of over a dozen murders and fifty sexual assaults in California over a ten year period, beginning in 1976.[19] DeAngelo was only arrested in 2018 after investigators uploaded crime scene samples to the consumer genealogical database GEDmatch, and were able to identify him by way of his distant relatives.[20]

Whereas privacy concerns are "difficult to quantify or demonstrate empirically", this visceral example illustrates the allure of this argument; police were able to arrest an offender responsible for abhorrent crimes, a tangible result from this new technology.[21] Professor Sonia Suter notes that "the social value of identifying murderers and rapists is palpable… it keeps them off the street, it provides peace and resolution to the victims and their families and it vindicates public justice."[22] Because apprehending offenders is easily recognised as beneficial, the public may be inclined to support the use of new investigative methods, regardless of the impact on human rights.

B Improved Efficiency

---

[17] *R (LS and Marper) v Chief Constable of South Yorkshire Police* (2004) UKHL 39, per Lord Steyn at [1].
[18] Ray Wickenheiser "Forensic genealogy, bioethics and the Golden State Killer case" (2019) 1 Forensic Science International 114 at 115.
[19] At 115.
[20] At 115.
[21] Sonia Suter "All in the Family: Privacy and DNA Familial Searching" (2010) 23 Harv J L & Tech 309 at 375.
[22] At 375.

CGS also provide significantly more genetic information than is stored on the current DNA databank. In New Zealand short tandem repeat (STR) analysis is used to create a DNA profile.[23] STR analysis can only identify close relatives, such as siblings or parents.[24] In comparison, CGS are much broader, as they utilise single-nucleotide polymorphisms, which can be used to identify ancestors.[25] One commentator described individuals becoming "a beacon who illuminates 300 people".[26] Additionally, it is "nearly costless for police to search CGS.[27] Consequently, searching CGS will make it less costly, and overall more efficient, for police to undertake genetic comparisons in the course of an investigation.

C Summary

Overall, it is impossible to ignore the benefits this technology may provide both police, and society more generally. This has been evidenced by the success of this technology overseas. However, the question becomes whether crime control is sufficient to justify undermining the right to privacy, and if so, how much state intrusion is too much?

IV Police Access to Consumer Genealogical Services: The Opposing Perspective

The following section will discuss the issues with police use of CGS, and conclude that despite the apparent benefits of this technology, unregulated use of these services will disproportionately interfere with the fundamental right to privacy.

A Breach of Individual Privacy

Various concerns have been raised in relation to CGS. Firstly, individuals who upload their data to CGS are subjected to preemptive surveillance by police. This is particularly concerning where the terms and conditions lack transparency about potential police access. Additionally, there is the issue that police searches of CGS are inconsistent with the purpose specification principle.

---

[23] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 190.
[24] At 190.
[25] At 190.
[26] Yaniv Erlich quoted in Benjamin Oreskes, Joseph Serna and Richard Winton "False starts in search for Golden State Killer reveal the pitfalls of DNA testing" (04 May 2018) Los Angeles Times <www.latimes.com>.
[27] Natalie Ram "Genetic Privacy After Carpenter" (2019) 105 Virginia L.Rev. 1357 at 1388.

1 Preemptive Surveillance of Innocent People

It has long been established that convicted offenders are not entitled to the same privacy rights as the rest of society due to their criminal activities.[28] This logic underpins the DNA databank, which contains the genetic information of known persons that can then be utilised in police investigations.[29]

However, police searches of CGS go far beyond what was envisioned by the DNA databank. Traditionally, to obtain further evidence against a person, police had to collect enough evidence to justify a search warrant. In what has been described as a "fishing expedition", CGS enable police to search a wide group of innocent people, effectively eliminating individuals until they find a suspect.[30] This raises serious privacy concerns; as one commentator put it, "everybody is under suspicion until we find the person who did it".[31]

Proponents of police searches of CGS may raise the "nothing to fear if you are innocent" argument. This suggests that innocent people should not object to having their information accessible to police.[32] However, this argument has been termed "fallacious", as it fails to consider the "harm, distress and stigma" associated with being involved in a criminal investigation.[33] This is particularly problematic in the context of CGS, as a person may be implicated by an incorrect genetic match. In the "Golden State Killer" investigation, GEDmatch produced two other suspects who were interviewed and swabbed by police.[34] These innocent people had to endure "the time, hassle and indignity" of being part of an investigation.[35] Overall, this argument does not convincingly invalidate the concern raised that police are surveilling innocent people.

2 Lack of Transparency in the Terms and Conditions

---

[28] Erin Murphy "Relative Doubt: Familial Searches of DNA Databases" (2009) 109 Mich L Rev 291 at 317-320.
[29] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 11.
[30] Oreskes, Serna and Winton, above n 26.
[31] Oreskes, Serna and Winton, above n 26.
[32] Nuffield Council on Bioethics *The Forensic Use of Bioinformation* (Nuffield Council on Bioethics, London, 2007) at 33.
[33] At 33.
[34] Oreskes, Serna and Winton, above n 26.
[35] David Kaye "The Genealogy Detectives: A Constitutional Analysis of Familial Searching" (2013) 50 Am Crim L Rev 110 at 156.

Another issue raised by these services is the lack of transparency in their contracts. Andelka Phillips has reviewed the contracts of 71 of these companies, which showed that many of these services contain "clickwrap" or "browse wrap" contracts.[36] Typically, a consumer purchasing an ancestry test would consent to the contract by merely clicking 'I Agree', without actually reading, or understanding, what they are agreeing to.[37]

These contracts are typically lengthy and complex, making them difficult for consumers to understand.[38] Because of how easy it is to accept the contract, and the complicated terms, consumers may fail to understand the privacy implications of submitting their DNA to these services.

Furthermore, consumers cannot negotiate the terms, which tend to be more favorable to the company than the consumer.[39] Phillips argues that CGS need to use more transparent terms to highlight the risks of uploading a DNA profile by making their contracts shorter, using simple language, or even providing videos explaining the risks and benefits to the consumer.[40]

However, because these sites are situated in overseas jurisdictions, regulation of their terms would be difficult, if not impossible. Nevertheless, the lack of transparency is indicative of the need for regulation of police access to these sites.

3 Failure to Accord with the Purpose Specification Principle

The purpose specification principle is the idea that data collected for one purpose cannot be used for another purpose unless consent is obtained.[41] According to the OECD guidelines, when personal data is collected, the purpose of collection "should be specified not later than at the time of data collection".[42] Any subsequent use of the data must be "limited to the fulfilment of those

[36] Andelka Phillips "Take an online DNA test and you could be revealing far more than you realise" (13 January 2016) The Conversation <www.theconversation.com>.
[37] Phillips "Take an online DNA test and you could be revealing far more than you realise" above n 36.
[38] Andelka Phillips *Genomic Privacy and Direct-to-Consumer Genetics* (Institute of Electrical and Electronics Engineers Security Workshop, New Jersey, 2015) at 61.
[39] Phillips "Take an online DNA test and you could be revealing far more than you realise" above n 36.
[40] Phillips *Genomic Privacy and Direct-to-Consumer Genetics,* above n 37, at 63.
[41] OECD "Core Privacy Principles" (2013) The OECD Guidelines at 9.
[42] At 9.

purposes or such others as are not incompatible with those purposes".[43] If the specified purpose is changed, the person whose data is being held needs to be notified.[44]

Police searches of CGS are incompatible with this principle. Data is uploaded by consumers for the purpose of discovering ancestors and ethnicity, rather than to help police investigations, and consumers have been given little or no chance to consent to this change of purpose.

For example, prior to the "Golden State Killer" investigation, GEDmatch did not mention the possibility of police accessing customer data.[45] Following the arrest of DeAngelo, privacy advocates raised concerns about the method of searching CGS. GEDmatch subsequently changed their privacy policy to give police access to their database for the purpose of investigating violent crimes.[46] Users were made aware of this change, and were given the option to agree.[47]

However, only months after this update, GEDmatch granted an exception by giving police access to their database to investigate an assault case.[48] This was outside the defined scope of "violent crime".[49] Contrary to the purpose specification principle, users were not made aware of this nor given a chance to consent to this exception.[50]

In response to public criticism, GEDmatch now gives users the ability to "opt in" to police searches.[51] While this may give the appearance of consent, as demonstrated above, these services can change the terms with ease, therefore the quality of this consent is questionable. Additionally, this is not the norm for these services, which typically rely on a standard disclosure clause stating they will release information to police if required.

---

[43] OECD, above n 41, at 9.
[44] At 9.
[45] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [9.113].
[46] GEDmatch.com "Terms of Service and Privacy Policy", above n 8.
[47] Ram, above n 27, at 1362.
[48] At 1362.
[49] At 1362.
[50] At 1362.
[51] Ram, above n 27, at 1363.

B Collective Privacy Concerns

Police searches of CGS also threaten collective privacy rights. Often, it has been assumed by policy makers that the rights of the individual will effectively "take care" of the rights of the group.[52] However, the development of new technology has led some scholars to argue that lawmakers need to start addressing group rights to privacy.[53]

Collective, or group privacy has been defined as "the right that is held by a group as a group rather than by its members severally. It is the group, not its members, that is correctly identified as the right-holder".[54] In other words, the group itself has a right to privacy. Dara Hallinan and Paul de Hert have observed that when a group's genetic data is being processed, it is the group as well as the individual whose rights are at risk.[55] Therefore, Hallinan and de Hert argue that the group "might be recognised as a separate subject of legal protection".[56]

However, despite increased recognition that group privacy should be subject to legal protection, New Zealand continues to uphold an individualised view of privacy, and therefore collective privacy has yet to make its way into any meaningful policy. In their 2010 review of the Privacy Act 1993, the Law Commission stated that it was:[57]

> ...hard to see how it [incorporating collective privacy into the Act] could work in practice… The Privacy Act is based on each individual's rights to control information relating to that individual, and it is very difficult to see how it could apply to groups without legal personality.

In the context of CGS, group privacy is relevant for two reasons: firstly there is the issue of the "genetic informant", as one person's DNA can implicate others who share genetic material.

---

[52] Luciano Floridi "Group Privacy: A Defence and an Interpretation" in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017) 83 at 97.
[53] See Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017).
[54] Floridi, above n 52, at 85.
[55] Hallinan and de Hert, above n 13, at 180.
[56] At 180.
[57] Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2010) at [3.81].

Secondly, because CGS hold whakapapa information, which Māori may consider belongs to a group as opposed to an individual.

1 The "Genetic Informant"

In effect, anyone who uploads their genetic data to one of these databases risks informing on their relatives without their knowledge or consent; essentially becoming a "genetic informant". One person's genetic profile can implicate a large group. One study estimated that 60 percent of searches for individuals of European descent will lead to a "third-cousin or closer match", and soon nearly every US individual with European descent could be implicated by these databases.[58]

Therefore, it is not only individual privacy interests which are threatened, but also the collective privacy interest of the group. This can result in unwanted scrutiny into that family, and depending on the culpability of the persons involved, may have long term impacts on familial relationships.[59]

One could argue that since these people have no knowledge their DNA is being searched, their privacy rights are not infringed. However, The Nuffield Council on Bioethics has stated that "the unauthorised use of such sensitive personal information might be seen as undermining the inherent dignity of human beings", regardless of whether there is "harm".[60] Therefore, irrespective of whether the individual knows about the search or not, the fact that it occurred at all results in a breach of privacy.

2 Concerns Raised in Relation to Tikanga Māori

Police searches of CGS also raise serious issues for tikanga Māori. DNA has whakapapa, which can be broadly described as genealogy.[61] Whakapapa is taonga, and is therefore subject to protection in accordance with Te Tiriti o Waitangi.[62] Police searches of CGS pose a risk to

[58] Yaniv Erlich and others "Identity inference of genomic data using long-range familial searches" (2018) 362 *Science* 690, at 690.
[59] Erica Haimes "Social and Ethical Issues in the Use of Familial Searching in Forensic Investigations: Insights from Family and Kinship Studies" (2006) 34 J.L.Med.& Ethics 263 at 269.
[60] Nuffield Council on Bioethics, above n 32, at 9.
[61] Hirini Moko Mead *Tikanga Māori: Living by Māori Values* (Revised Edition, Huia Publishers, Wellington 2016), at 41.
[62] *New Zealand Māori Council v Attorney-General* [1994] 1 NZLR 513 (PC) at [517].

whakapapa, as they might reveal information about genetic relationships that was previously unknown. For example, individuals have used the site to find biological parents or sperm donors.[63]

In their *Stage One Review of the Law of Privacy*, the Law Commission found that making whakapapa information available online could be "seen as violating tapu, breaching protocols surrounding oral transmission of knowledge, and placing information at risk of misuse by people seeking to claim rights based on fabricated whakapapa connections".[64] However, placing whakapapa information online may also allow individuals "to learn about their history and ancestry, and to reconnect with their whānau, hapū and iwi".[65] This finding by the Law Commission was supported by reference to the website Māori.org.nz, which created a whakapapa section on their website to connect people to their whānau.[66]

In the Family Court case *GM, Re To adopt a child,* the issue was whether whakapapa information should be published by the court.[67] In that case, Associate Professor Thomas Roa, an expert in Māori and indigenous studies, stated that whakapapa should only be made public if the whānau gives permission, and are aware of who may access it.[68] The discussion earlier in this chapter demonstrated how CGS often lack transparency in their contracts, which could result in individuals uploading their genetic data unaware that police may access it.

Where whakapapa information has been uploaded to CGS, reservations have been raised as to whether police should have access to it. Karaitiana Taiuru submitted to the Law Commission that while uploading information to such sites would compromise the tapu of the DNA, there are still "serious concerns" with permitting the police to search CGS.[69] Te Mana Raraunga, the Māori Data Sovereignty Network, opposed this technique altogether, as allowing police to search CGS would

---

[63] Thomas Brewster "Why Sperm Donor Privacy Is Under Threat From DNA Sites—Is There Anything They Can Do About It?" (23 April 2019) Forbes <www.forbes.com>.
[64] Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008), at [5.30].
[65] At [5.30].
[66] Māori.org.nz "Should Whakapapa be Online?" <www.māori.org.nz>.
[67] *GM, Re To adopt a child* [2018] NZFC 3915 at [12].
[68] At [13].
[69] Taiuru Māori "Submission to the Law Commission: DNA in Criminal Investigations" <https://www.taiuru.maori.nz>.

also breach Māori data sovereignty, under which the use and collection of data pertaining to Māori would be governed by Māori.[70]

Māori may consider that certain types of personal information belong to the group, rather than to the individual. One example of this is whakapapa information. Access to whakapapa information is "carefully guarded, and custodians of whakapapa hold it on behalf of their whānau, hapū or iwi".[71] This information relates to a group, not an individual. Therefore, "the impact upon a breach of privacy for a Māori isn't only ever about that individual, it is always about their familial ties and their community connection or their local geography".[72] A report to the States Services Commission noted that:[73]

> The issue of "collective ownership" and "collective privacy" incorporates the idea of a whānau or hapū "owning" their collective information also referred to as aggregated or statistical data. This enables their rights to make decisions about that information including how it is shared, how it is aggregated and how it is published.

Consequently, privacy protections which focus on the individual are insufficient to uphold Māori interests. This issue can be illustrated by reference to CGS, however collective privacy in Māori genetic data is a broader issue beyond the scope of this paper.

C Summary of the Privacy Implications

This chapter has demonstrated that permitting police to search CGS would infringe not only on individual privacy rights, but also the rights of the collective who are brought into an investigation due to shared genetic material. Despite these concerns, the following chapter will demonstrate that there are limited protections from police searches of CGS under the existing law.

---

[70] Donna Cormack *Submission on the Law Commission Review of the Law Governing the use of DNA in Criminal Investigations in New Zealand* (April 2019) at 13.
[71] Law Commission *Privacy Concepts and Issues,* above n 64, at [5.28].
[72] Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/Broadcasting Standards Authority, Wellington, 2004) at 57.
[73] Paua Interface Ltd Research of Issues for Māori Relating to the Online Authentication Project (report for the State Services Commission, 2004) at 23.

V Protections Under the Existing Law

Given the issues with police searches of CGS, the question becomes whether, without regulation, New Zealand consumers would be protected under the current law? The following chapter will examine the Privacy Act 1993 (the Act) and the New Zealand Bill of Rights Act 1990 (NZBORA) to illustrate that there is limited protection for consumers from police searching their genetic information.

The current law in regards to the relationship between s 21 of NZBORA and the Privacy Act was articulated in the recent Supreme Court case of *R v Alsford*.[74] This case provides a useful analogy to CGS because police sought voluntary disclosure of customer information from a third party service provider.[75] Because there is currently no case law pertaining to CGS, this analogy will be used to demonstrate how the existing law would likely apply to CGS.

A The Role of the Privacy Act 1993

The purpose of the Privacy Act is to "promote and protect individual privacy".[76] To do this, the Act established principles relating to:[77]

1. The collection, use, and disclosure of information relating to individuals; and
2. access by individuals to information held about them.

The Act applies to "personal information", which is defined as "information about an identifiable individual."[78] "Individual" is described as "a natural person, other than a deceased person."[79] Evidently, the Act is largely focused on protecting individual rights to privacy.

The Act also contains twelve information privacy principles which deal with the "collection, holding, use and disclosure of personal information".[80] These principles are not enforceable in a

[74] *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR 710.
[75] At [7].
[76] Privacy Act 1993, long title.
[77] Privacy Act, long title.
[78] Section 2.
[79] Section 2.
[80] Law Commission *Protecting Personal Information From Disclosure* (NZLC PP49, 2002), at 2.

court of law.[81] This is because the Act aims to promote voluntary compliance.[82] If an individual feels the privacy principles have been breached, they can make a complaint to the Privacy Commissioner.[83]

The following section will demonstrate that police searches of CGS would likely be protected by principle 11(d) or alternatively principle 11(e)(i). However, as noted above, a finding that the use of CGS amounted to a breach of the Act is not enforceable by the courts.[84]

1 Exception under Principle 11(d): Authorisation by the Individual

When police request information from a third party as part of an investigation, they must comply with the Privacy Act, which prohibits disclosure of personal information.[85] However, there are exceptions to this prohibition, one of which is where disclosure is authorised by the individual.[86]

If the consumer genealogical service allows consumers to consent to police searching their genetic data, the service will likely be able to release information to police relying on principle 11(d).[87] Under this principle, the agency must believe on reasonable grounds that the individual concerned consented to the release of the information.[88] This test would be easily satisfied where the contract allows consumers to "opt in" to police searches.

However, currently the only service which has this "opt in " provision is GEDmatch. Other CGS rely on standard disclosure clauses which state that they may release customer information to police. This exception may not be satisfied where the terms merely contain a disclaimer that there is a possibility their information will be released.[89] In this situation, police would have to rely on Principle 11(e)(i).

---

[81] Privacy Act 1993, s 11.
[82] Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123, 2011), at [6.2].
[83] Privacy Act, s 67.
[84] Section 11.
[85] Section 6.
[86] Section 6, cl 11.
[87] GEDmatch.com, above n 8.
[88] Privacy Act, s 6, cl 11.
[89] See Ancestry.com "Your Privacy" <www.ancestry.com>.

2 Maintenance of the Law Exception

Principle (11)(e)(i) provides another exception to the general prohibition on disclosure, it states:

> An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—
> …
> (e) that non compliance is necessary—
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences

This section gives police officers the ability to seek customer information from organisations voluntarily, as long as it is to prevent prejudice of the maintenance of law. It is up to the service to decide whether to release the information, however they must be able to justify why they disclosed the information.[90] Therefore, police must provide sufficient information to enable the service provider to determine whether disclosure is "necessary" for the purposes of principle 11(e)(i).[91]

In *Alsford*, maintenance of law was given a broad definition. Arnold J stated that the wording of the statute "suggests that the test – belief on reasonable grounds that non-compliance is necessary – is a relatively low one".[92] Therefore, so long as the information sought is in the course of an investigation, this exception would be satisfied.

Applying this to CGS, police could request information relying on principle 11(e)(i). The service would then need to be satisfied that they have reasonable grounds to believe that releasing the information is necessary to avoid prejudice to the maintenance of the law. If this is satisfied there will be no breach of s 11(e)(i).

However, if the information was released by the service, and the court determined it was in breach of principle 11(e)(i), this would not necessarily result in a finding against the police. In *Alsford,*

---

[90] *R v Alsford,* above n 74, at [42].
[91] At [35].
[92] At [34].

the court determined while there was a breach of the privacy principles there was no breach of s 21 of NZBORA, and therefore the majority did not find in the claimants favour.[93]

B Can NZBORA Protect Voluntarily Uploaded Genetic Information?

Section 21 of the NZBORA states that "everyone has the right to be secure against unreasonable search or seizure".[94] The following section will examine the current approach to s 21, which will illustrate that the NZBORA fails to confer any real protection on genetic data held by CGS.

1 The Court's Interpretation of Section 21: R v Alsford

Whether there was a "search" for the purposes of s 21 depends on whether the individual had a subjective expectation that the information would be kept private, and if so whether that expectation was objectively reasonable. This objective element provides a check on the subjective expectation of the individual.[95] It also requires the court to take into consideration the circumstances of the case to come to a conclusion as to whether the expectation was reasonable.[96] This aims to protect the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state" and includes information "which tends to reveal intimate details of the lifestyle and personal choices of the individual".[97]

The reasonable expectation of privacy test was articulated by Blanchard J in *Hamed v R.* In deciding the case, Blanchard J adopted the two stage test from *Katz v United States*.[98] In *Katz*, it was determined that a complaint has a reasonable expectation of privacy where:[99]

> (1) the complainant subjectively held an expectation of privacy and,
>
> (2) that subjective expectation was one that society is prepared to recognise as reasonable.

---

[93] *R v Alsford,* above n 74, at [100].
[94] New Zealand Bill of Rights Act 1990, s 21.
[95] N.A. Moreham "Unpacking the reasonable expectation of privacy test" (2018) 134 L.Q.R. 651 at 654.
[96] *R v Alsford,* above n 74, at [63].
[97] At [56], citing *R v Plant* [1993] 3 SCR 28 at 292.
[98] *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163], citing Katz, above n 13 at [361].
[99] *Katz v United States* 389 US 347 (1967) at [361].

Blanchard J's approach was upheld by the majority of the Supreme Court in *Alsford,* and therefore embodies the current approach as to whether there was an "unreasonable search" for the purposes of s 21.[100]

2 Applying R v Alsford *to Police Searches of Consumer Genealogical Services*

In order to establish whether an individual's expectation of privacy was reasonable, the court will take into consideration a range of factors.[101] In *Alford,* the majority ascertained, based on Canadian authorities, four relevant factors:[102]

(a) the nature of the information at issue;
(b) the nature of the relationship between the party releasing the information and the party claiming confidentiality in the information;
(c) the place where the information was obtained; and
(d) the manner in which the information was obtained.

The information in question is DNA, and is therefore highly sensitive and deeply revealing. Ostensibly it is the type of information that s 21 would want to prevent intrusion into. However, information that is voluntarily shared and available on the internet is generally considered to have a "low reasonable expectation of privacy".[103] GEDmatch allows users to upload their DNA profile and then search the database for a genetic match. Their privacy policy states that "if you require absolute privacy and security, we must ask that you do not upload your data to GEDmatch".[104] Therefore, individuals upload their data to GEDmatch with the knowledge that this information will be accessible to anyone who uses this service.

(a) Relevance of Disclosure Clauses

[100] *R v Alsford,* above n 74, at [50].
[101] At [63].
[102] At [63].
[103] William Fussey "Determining Reasonable Expectation of Privacy in the Intrusion into Seclusion Tort" (2016) 22 Canterbury L.Rev 269 at 283.
[104] GEDmatch.com "Terms of Service and Privacy Policy", above n 8.

In *Alsford*, the court stated that the terms and conditions did not "advance matters much, if at all".[105] This was because two of the policies in question stated that they may release customer information in accordance with the Privacy Act 1993. This indicated that Mr Alsford's expectation of privacy was not reasonable.[106] However, one of the policies stated they would only release customer information if they were "legally required to".[107] This indicated that the service would only release the information if a warrant or production order was obtained.[108] This supported Mr Alsford having a reasonable expectation of privacy, as he could fairly assume police would need to obtain a warrant or production order to access the information, which they did not.[109]

Whether the complaint held a reasonable expectation of privacy may therefore depend on what type of clause was contained in the contract, and how transparent it was. For example, the "opt in" clause included in the GEDmatch terms and conditions would make it difficult for an individual to argue they had a reasonable expectation of privacy in the data, as they essentially permitted disclosure. However, 23andMe will only disclose information if required by a court order, subpoena or a warrant.[110] Ancestry.com's privacy statement states that it will only cooperate with police where they are following a "valid legal process".[111] These clauses may point towards an individual having a reasonable expectation of privacy in the information, as one may expect the police to obtain a search warrant or production order before accessing these sites.

The transparency of these terms and conditions may also factor into the analysis. While many of these services do contain a disclosure clause, this may often be overlooked by the individual uploading their data. This would point towards there being a reasonable expectation of privacy. However, it could be argued that the fact the terms and conditions contemplate disclosure indicates that any expectation of privacy was not reasonably held.

(b) Compliance with the Privacy Act 1993

---

[105] *R v Alsford,* above n 74, at [71].
[106] At [71].
[107] At [71].
[108] At [71].
[109] At [71].
[110] 23andme "Privacy Highlights" <www.23andme.com>.
[111] Ancestry.com "Your Privacy", above n 89.

Compliance with the privacy principles may also inform whether there was an unlawful search for the purposes of s 21.[112] If a court found that the disclosure was compliant with the privacy principles they may be more willing to hold that there was no breach of s 21. However, a breach of the privacy principles will not determine whether there was a breach of s 21.[113] Therefore, even if disclosing the information was in breach of the privacy principles, this would not necessitate a finding that there was a breach of s 21.

(c) Summary on Reasonable Expectation of Privacy

Ultimately, despite the deeply revealing nature of the information in question, it is unlikely it would be protected by s 21 without specific legislative reform. The opt-in provision and the fact that it is publicly accessible makes it clear that users who upload to GEDmatch would not have a reasonable expectation of privacy in the information.

A breach of s 21 of NZBORA may be more arguable if police were to search sites such as Ancestry.com or 23andme.com, as these services do not permit public access to users' genetic data and only contemplate possible disclosure to police. However, individuals do upload their data voluntarily, and the terms do mention possible disclosure. Additionally, police may be able to seek voluntary disclosure under principle 11(e)(i) of the Privacy Act,. If police were compliant with principle 11(e)(i), this would point towards there being no breach of s 21. Therefore it is still entirely possible the court would find that there was no reasonable expectation of privacy in information uploaded to these services.

Currently there are no decisions on this issue in New Zealand, however the finding that there would not be a reasonable expectation of privacy was supported by the Law Commission in their report *DNA in Criminal Investigations.*[114]

VI Policy Considerations

---

[112] *R v Alsford,* above n 74, at [64].
[113] At [64].
[114] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [9.117].

It is clear from the preceding discussion that regulation is necessary to protect both individual and collective privacy from invasion by police searches of CGS. This chapter will examine the policy objectives which would underlie any reform. Reform options will then be assessed against how well they achieve these policy considerations.

A Competing Aims

These services hold vast amounts of DNA, and therefore have the potential to be an invaluable resource in police investigations. However, as discussed in Chapter IV, significant privacy risks arise where police search CGS. Therefore, the societal benefit of apprehending offenders will need to be balanced against the right to privacy; two laudable but competing aims.

B Why is Regulation Necessary?

Because of the jurisdictional issue that arises in the context of CGS, any reform would have to focus on regulating police access to them.

The New Zealand Police currently claim they have no intention of using the data stored by CGS, although they have made "inquiries" into how these sites may be used in an investigation.[115] Given the trend towards expanding DNA databanks, the temptation to use CGS may become irresistible, especially considering the success of this technology in other jurisdictions.

If police utilise CGS, neither the Privacy Act nor the NZBORA confers any real protections on individual or collective privacy. Therefore, both the individual and the group will have to rely on the sites themselves to protect their genetic information. According to the transparency reports released by Ancestroy.com and 23andme.com, there have been no successful requests made by law enforcement to obtain information held by these services.[116] Prima facie this may give consumers peace of mind that their data is protected.

However, it is questionable how long such privacy interests will be upheld. As discussed in Chapter IV, these services can simply update their terms and conditions, often with little or no

[115] Brittany Keogh "Police Make Inquiries Aboute Using DNA from Ancestory.com to Solve Crime" (03 November 2019) Stuff <www.stuff.co.nz>.
[116] Ancestry.com "Your Privacy" above n 89. See also 23andme, above n 110.

consent from the consumers. For example, Ancestry.com "reserve[s] the right to change the Ancestry entity which is a party to these Terms at any time", and they "may" contact consumers with any changes.[117] 23andme.com has a similarly worded clause which allows them to change the terms and conditions, and consumers may or may not be directly informed.[118]

Ultimately, the risk with relying on these sites to protect consumer's genetic information is that their terms and conditions are subject to change. Therefore, despite their current stance limiting access to police, it is possible these sites will choose to cooperate with law enforcement in future.

C Regulatory Options: Mitigating the Risks

The following discussion will outline three different methods of regulating police searches of CGS; prohibition, establishing a universal database, or dedicated regulation of police actions. The most desirable reform option will be decided on how well it balances the competing aims outlined above.

1 Prohibit Police Searches of Consumer Genealogical Services

One option for reform is banning these searches through legislation. While a complete ban would alleviate the issues discussed in Chapter IV, police investigations would be unnecessarily hampered. Ultimately, the concerns raised in regard to CGS could be mitigated without banning police searches altogether.

2 Establish a Universal Database

Another option for reform is to establish a universal database, in which every person's DNA was held and available for use by police. This would make it unnecessary for police to search CGS, as they would have access to a population wide database. While the Law Commission did discuss the possibility of establishing a universal database in their report *DNA in Criminal Investigations*, they did not favour such a recommendation.[119]

---

[117] Ancestry.com "Your Privacy", above n 89.
[118] 23andme, above n 110.
[119] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 255-258.

Establishing a universal database would be a clear example of "function creep", which describes "how a government's program of technological intervention into social life is gradually, incrementally, but deliberately, increased over time."[120] A universal database would be a significant expansion on what DNA is currently available to police. Therefore, while this would make it unnecessary for police to use CGS, it inappropriately impedes on the right to privacy and is ultimately disproportionate to the need to solve crime.[121]

3 Dedicated Regulation of Police Activities

Lastly, regulation could take a more balanced approach, which would permit searches of CGS while putting procedures in place to regulate police activities. Dedicated guidance of police behaviour is the most favourable reform option, as unlike a ban or universal database, it balances the two competing aims of apprehending criminals while also minimising the potential for abuse.

The question then becomes how to best regulate police behavior to ensure individual and group privacy rights are protected? This will be discussed in the following chapter.

VII How to Best Regulate Police Searches of Consumer Genealogical Services

Broadly, there are two possible routes to regulate police behaviour. Firstly, there is a rule based approach, under which police behavior would be governed by legislation, a policy statement, or both. Secondly, police activities could be subject to external oversight.

The following section will illustrate that a combination of these approaches will allow police to utilise this technology in a restricted set of circumstances, while also minimising the opportunities for abuse.

A A Rules Based Approach

[120] Robin Williams and Paul Johnson *Genetic Policing: The use of DNA in Criminal Investigations* (Willan Publishing, Devon, 2008) at 82.
[121] Nuffield Council on Bioethics, above n 32, at 59.

One way to regulate police behaviour is through rules which restrict the circumstances in which police can search CGS. This could take the form of one of a policy statement or specific legislation. These options will be discussed in detail in the following sections.

1 Develop a Policy Statement

One option to regulate police behaviour is to permit searches of CGS, but limit it under a policy statement developed by the Police. Policy statements are similar to "a code of conduct or code of practice. They... give guidance on best practice".[122] This would give police definite instructions on whether their search is lawful. If it is, this would minimise the risk of a court finding that it breached s 21 of NZBORA, or of evidence being excluded.[123] Policy statements are also accessible to the public, which increases "consistency, transparency and accountability".[124]

Flexibility is inherent in policy statements, as police have the ability to regularly review and change the policy depending on societal needs.[125] However, this flexibility comes with the risk of "function creep", as police may over time incrementally expand the situations in which they use CGS. Consequently, policy statements do not "provide the same level of clarity, safeguards or oversight that a warrant system or oversight body would provide."[126]

Overall, it would be advantageous to outline the more technical aspects of police searches in a policy statement. This would allow police to update their methods and protocols as technology advances, without the need for legislative change. Accordingly, a policy statement might still be beneficial where it was used alongside legislation and external oversight.

2 Permitting Police to Search Consumer Genealogical Services

---

[122] Law Commission *Review of the Search and Surveillance Act 2012 Ko te Arotake i te Search and Surveillance Act 2012* (NZLC IR141, 2018) at [5.17].
[123] At [5.18].
[124] At [14.65].
[125] At [5.37].
[126] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [9.108].

Permitting police to search CGS through legislation is another option to regulate police behaviour. A provision could be inserted into the CIBS Act, which would clearly establish in what circumstances police could search CGS, and what limitations they would be subject to.

Ultimately, a restrictive approach is necessary in order to protect privacy rights. Therefore, police should only access CGS for violent crimes, or to identify a missing person or human remains.[127] What constitutes a violent crime would need to be explicitly defined to prevent a "function creep", where police access CGS for an increasing range of crimes contrary to the original intention of the rule.

Additionally, police searches of CGS could be limited to situations in which traditional investigative methods have failed to produce any leads. For example, police would first have to search the DNA databank of known offenders. If this failed to produce a match, and other investigative methods were also unlikely to produce a viable result, then police may use CGS. However, again it would need to be clearly defined at what point access to CGS would be permitted.

The benefit of legislative reform is that a statute provides certainty missing from a policy statement. This would prevent police expanding their powers unless there is extensive public support for such a change.

B External Oversight

Legislative change and a policy statement would act jointly to provide clarity and certainty on police use of CGS, however these would only be effective at protecting rights if they are subject to external scrutiny.

The Forensic Genetics Policy Initiative observed that:[128]

[127] The United States Department of Justice, above n 9.

[128] Forensic Genetics Policy Initiative *Establishing Best Practice for Forensic DNA Databases* (September 2017) at 25.

> Best practice for DNA databases includes an independent and transparent system of governance with regular information published… There must be adequate public and regulatory scrutiny to ensure the database is compliant with the law and to maintain public confidence.

This is consistent with findings by the Nuffield Council over ten years ago, which found:[129]

> ...the potential uses and abuses of forensic databases are considerable. Effective governance helps to ensure not only that their utility is maximised, but also that their potentially harmful effects – such as threatening privacy, undermining social cohesion and aggravating discriminatory practices – are minimised.

Considering these findings, it is clear that external oversight is necessary to ensure privacy rights are not being abused in the course of police investigations. This could be done in one of two ways: judicial oversight or an independent oversight body.

1 Independent Oversight Body

The Law Commission has acknowledged that there are various benefits in establishing an external oversight body to oversee the use of DNA in police investigations.[130] These benefits include the preservation of public understanding, trust and engagement, as well as minimising harms and potential miscarriages of justice.[131] Given the complexities of DNA and the various interests at stake, an external oversight body would need to be specialised. It is also important that Māori have a central position in the decision-making process to ensure police act consistently with tikanga and the Te Tiriti o Waitangi.

An oversight body would mitigate many of the issues raised in regards to these services by ensuring police act in accordance with the legislation, which would be drafted with a focus on protecting privacy rights. Additionally, it could assist in a broad range of activities. For example, it would be

---

[129] Nuffield Council on Bioethics, above n 32, at [7.1].
[130] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 339.
[131] At 339.

able to respond to specific complaints and approve police activities.[132] It could also advise on policy, undertake public education initiatives and ensure police comply with any statutory powers.[133] An oversight body could also protect collective privacy interests pertaining to DNA.

Specifically legislating for a restricted use of CGS, or establishing an independent oversight body, would minimise the risk to collective privacy where police search these services, as police could only search these services in limited circumstances. Therefore, it is arguable that including group privacy into the Privacy Act, or another piece of legislation, would be unnecessary. However, Chapter IV demonstrated that Western understandings of privacy do not adequately protect Māori interests. Moving forward, there needs to be greater discussion as to how collective privacy could be incorporated into New Zealand law, regardless of whether there is reform relating specifically to CGS, this is a broader discussion to be had beyond CGS.

2 Judicial Oversight

Finally, police searches of CGS could be subjected to judicial oversight. Legislation could be enacted which requires police to obtain a warrant or production order before a search is authorised.

Requiring police to obtain a warrant is more in line with traditional investigative techniques, as it would require the police to build a case against a person before embarking on a search of CGS. This would mitigate the risk of police undertaking a "fishing expectation" to find suspects. Additionally, because the use of CGS would be limited to a specific set of circumstances, requiring judicial oversight should not overly burden the courts.

The argument against this approach is that it would be overly time consuming and could stifle investigations where police have insufficient information to obtain a warrant or production order, thus leading to unsolved cases.

---

[132] At 339.

[133] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at 339.

However, Elias CJ in *Alsford* observed that where police seek voluntary disclosure, they need to be able to "identify why obtaining a production order or search warrant would prejudice the investigation".[134] Where police have insufficient information to obtain a warrant or production order, they might seek voluntary disclosure. However, her Honour did not consider this to be an adequate justification for failing to obtain a warrant or production order.[135] According to her Honour's reasoning, urgency might legitimize police failing to obtain a court order to search a consumer genealogical service, however insufficient information would not.

In addition, the potential risks to privacy make the argument that it is overly time consuming alone is insufficient to justify police circumventing court oversight.

Overall, while it may be more somewhat burdensome for police to obtain a warrant or production order, this is an acceptable price to pay to ensure the right to privacy is protected.

C Regulating Police Behaviour: Summary

A policy statement is more flexible than legislation. Given the ever changing nature of DNA technology, a policy statement could be used to regulate the technical rules and procedures police need to follow when searching CGS. This would allow police to stay updated with any future developments.

However, this would need to be supplemented by legislation which would explicitly outline when police can search CGS. This would help to minimise the risk of a "function creep", as any amendments would be subject to public scrutiny.

This rules based approach would still need to be accompanied by a form of external oversight, which would ensure that police activities are compliant with any legislation, and that privacy rights are not being violated for investigative purposes.

---

[134] *R v Alsford,* above n 74, at [184].
[135] At [184].

External supervision could be in the form of an independent body, judicial oversight, or both. Subjecting police activities to judicial oversight would limit the risk of police abusing this technology, as they would need to obtain judicial consent before undertaking a search. However, the benefit of an independent oversight body is that it can be specialised, and undertake a broader range of activities aimed at protecting privacy interest. Overall, an external overnight would be able to take on many functions aimed at upholding human rights.

Ultimately, permitting police to search such a vast database is a significant expansion of their current powers, and as such needs to be accompanied by some form of oversight to minimise the risk of this power being misused.

VIII Conclusion

It is undeniable that DNA technology has transformed police investigations. Its reliability has seen it termed the "gold standard" of forensic science, and it has allowed police to arrest and prosecute individuals who may have otherwise evaded identification.[136] Therefore, it is unsurprising that the DNA databank has continued to expand over the years since its inception.

But how far is too far? CGS would essentially conform to this tendency by increasing the amount of genetic information police can access. However, these services go far beyond what information is currently contained in the DNA databank.

Overseas, CGS have allowed police to apprehend violent offenders who likely would have avoided prosecution had these services not been available. This is a compelling argument in favour of allowing these searches, as one commentator put it, "Why... would we come up with a reason that we not be able to use it, on the argument that it intrudes onto *[sic]* someone's privacy?".[137]

---

[136] Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara,* above n 1, at [2.13].

[137] Josh Marquis quoted in Justin Jouvenal and others "Data on a genealogy site led police to the 'Golden State Killer' suspect. Now others worry about a 'treasure trove of data'" (28 April 2018) Washington Post <www.washingtonpost.com>.

However, CGS also subject innocent people to genetic surveillance. This erosion of privacy rights necessitates limitations on when police can use CGS. In 1992, Judge Murnaghan, in the US Court of Appeals, made the pertinent observation that:[138]

> The majority opinion [that the DNA databank was constitutional]... leads me to a deep, disturbing, and overriding concern that, without a proper and compelling justification, the Commonwealth may be successful in taking significant strides towards the establishment of a future police state, in which broad and vague concerns for administrative efficiency will serve to support substantial intrusions into the privacy of citizens.

Ultimately, regardless of investigative efficiency, privacy rights require active protection from unwarranted state surveillance in order to uphold human dignity and autonomy.

[138] *Jones v. Murray* 962 F.2d. 302 at [313].

IX Bibliography

A Cases

1 New Zealand

GM, Re To adopt a child [2018] NZFC 3915.

Hamed v R [2011] NZSC 101, [2012] 2 NZLR 305.

New Zealand Māori Council v Attorney-General [1994] 1 NZLR 513 (PC).

R v Alsford [2017] NZSC 42, [2017] 1 NZLR 710.

2 England

R (LS and Marper) v Chief Constable of South Yorkshire Police (2004) UKHL 39.

3 Canada

R v Plant [1993] 3 SCR 28.

4 United States of America

Jones v. Murray 962 F.2d. 302.

Katz v United States 389 US 347 (1967) .

B Legislation

Criminal Investigations (Bodily Samples) Amendment Act 2003.

Criminal Investigations (Bodily Samples) Amendment Act 2009.

New Zealand Bill of Rights Act 1990.

Privacy Act 1993.

C Books and Chapters in Books

Broadcasting Standards Authority *Real Media, Real People: Privacy and Informed Consent in Broadcasting* (Dunmore Press/Broadcasting Standards Authority, Wellington, 2004).

Luciano Floridi "Group Privacy: A Defence and an Interpretation" in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017) 83.

Dara Hallinan and Paul de Hert "Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law" in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017) 175.

Hirini Moko Mead *Tikanga Māori: Living by Māori Values* (Revised Edition, Huia Publishers, Wellington 2016).

Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) *Group Privacy* (Springer International Publishing, Switzerland, 2017).

Robin Williams and Paul Johnson *Genetic Policing: The use of DNA in Criminal Investigations* (Willan Publishing, Devon, 2008).

D Journal Articles

Yaniv Erlich and others "Identity inference of genomic data using long-range familial searches" (2018) 362 *Science* 690.

William Fussey "Determining Reasonable Expectation of Privacy in the Intrusion into Seclusion Tort" (2016) 22 Canterbury L.Rev 269.

Erica Haimes "Social and Ethical Issues in the Use of Familial Searching in Forensic Investigations: Insights from Family and Kinship Studies" (2006) 34 J.L.Med.& Ethics 263.

David Kaye "The Genealogy Detectives: A Constitutional Analysis of Familial Searching" (2013) 50 Am Crim L Rev 110.

N.A. Moreham "Unpacking the reasonable expectation of privacy test" (2018) 134 L.Q.R. 651.

Erin Murphy "Relative Doubt: Familial Searches of DNA Databases" (2009) 109 Mich L Rev 291.

Natalie Ram "Genetic Privacy After Carpenter" (2019) 105 Virginia L.Rev. 1357.

Sonia Suter "All in the Family: Privacy and DNA Familial Searching" (2010) 23 Harv J L & Tech 309.

Ray Wickenheiser "Forensic genealogy, bioethics and the Golden State Killer case" (2019) 1 Forensic Science International 114.

E Parliamentary and government materials

Law Commission *Privacy Concepts and Issues* (NZLC SP19, 2008).

Law Commission *Protecting Personal Information From Disclosure* (NZLC PP49, 2002).

Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2010).

Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123, 2011).

Law Commission *Review of the Search and Surveillance Act 2012 Ko te Arotake i te Search and Surveillance Act 2012* (NZLC IR141, 2018)

Law Commission *The Use of DNA in Criminal Investigations. Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* (NZLC IP43, 2018).

F Reports

Forensic Genetics Policy Initiative *Establishing Best Practice for Forensic DNA Databases* (September 2017).

Nuffield Council on Bioethics *The Forensic Use of Bioinformation* (Nuffield Council on Bioethics, London, 2007).

Paua Interface Ltd Research of Issues for Māori Relating to the Online Authentication Project (report for the State Services Commission, 2004).

Andelka Phillips *Genomic Privacy and Direct-to-Consumer Genetics* (Institute of Electrical and Electronics Engineers Security Workshop, New Jersey, 2015) .

G Internet Resources

23andme "Privacy Highlights" <www.23andme.com>.

Ancestry.com "Ancestry - Home" <www.ancestry.com>.

Ancestry.com "About Us - Overview" <www.ancestry.com>.

Ancestry.com "Your Privacy" <www.ancestry.com>.

Thomas Brewster "Why Sperm Donor Privacy Is Under Threat From DNA Sites—Is There Anything They Can Do About It?" (23 April 2019) Forbes <www.forbes.com>.

GEDmatch.com "Terms of Service and Privacy Policy" (20 May 2018) <www.gedmatch.com>.

Jocelyn Kaiser "We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans" (11 October 2018) Science <www.sciencemag.org>.

Brittany Keogh “Police Make Inquiries Aboute Using DNA from Ancestory.com to Solve Crime” (03 November 2019) Stuff <www.stuff.co.nz>.

Māori.org.nz “Should Whakapapa be Online?” <www.māori.org.nz>.

Josh Marquis quoted in Justin Jouvenal and others “Data on a genealogy site led police to the ‘Golden State Killer’ suspect. Now others worry about a ‘treasure trove of data’” (28 April 2018) Washington Post <www.washingtonpost.com>.

Andelka Phillips “Take an online DNA test and you could be revealing far more than you realise” (13 January 2016) The Conversation <www.theconversation.com>.

Taiuru Māori “Submission to the Law Commission: DNA in Criminal Investigations” <https://www.taiuru.maori.nz>.

H Other resources

Donna Cormack *Submission on the Law Commission Review of the Law Governing the use of DNA in Criminal Investigations in New Zealand* (April 2019).

OECD “Core Privacy Principles” (2013) The OECD Guidelines.

The United States Department of Justice “Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes” (press release, 24 September 2019).

Word count

The text of this paper (excluding table of contents, footnotes, abstract and bibliography) comprises approximately 7, 902 words.