Marcus Smith • Seumas Miller

Biometric Identification, Law and Ethics

Springer

Marcus Smith
Charles Sturt University
Canberra, ACT, Australia

Seumas Miller
Charles Sturt University
Canberra, ACT, Australia

TU Delft
Delft, The Netherlands

University of Oxford
Oxford, UK

The research was conducted under the auspices of: (i) the European Research Council's Advanced Grant programme as part of the grant entitled, "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller) and (ii) the Australian Research Council's Discovery Grant program as part of the grant entitled, "Intelligence and National Security: Ethics, Efficacy and Accountability" (DP180103439).

ISSN 2211-8101 ISSN 2211-811X (electronic)
SpringerBriefs in Ethics
ISBN 978-3-030-90255-1 ISBN 978-3-030-90256-8 (eBook)
https://doi.org/10.1007/978-3-030-90256-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgement

The research was conducted under the auspices of: (i) the European Research Council's Advanced Grant program as part of the grant entitled "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller) and (ii) the Australian Research Council's Discovery Grant program as part of the grant entitled "Intelligence and National Security: Ethics, Efficacy and Accountability" (DP180103439).

Contents

About the Authors

Marcus Smith is Associate Professor in Law at Charles Sturt University and Adjunct Professor of Law at the University of Canberra. He holds a PhD in law from the Australian National University. He has published widely on technology law, regulation and ethics. His previous books include: *Technology Law* (Cambridge University Press, 2021), *Biometrics, Crime and Security* (Routledge, 2018) and *DNA Evidence in the Australian Legal System* (LexisNexis, 2016).

Seumas Miller has research appointments at Charles Sturt University, TU Delft and the University of Oxford. He is the principal investigator on a European Research Council Advanced Grant on counter-terrorism ethics, and is the author of more than 200 academic articles and 20 books, including *The Ethics of Cybersecurity* (with Terry Bossomaier) (Oxford University Press, 2021) and *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (Springer, 2018).

Chapter 3
DNA Identification, Joint Rights and Collective Responsibility

Abstract DNA identification developed late in the twentieth century and has surpassed fingerprinting as the leading technique for forensic human identification. It differs from the other biometrics discussed in that it is based on principles of biological, rather than physical sciences. Another difference is the time taken to convert a biological sample into a DNA profile; however, this is becoming less significant as technology progresses. DNA is also more accurate and revealing in comparison with other biometrics because it can provide information about a person's physical appearance and health status, as well as link an individual to, and in association with further investigations, identify, their biological relatives. This chapter examines DNA identification in law enforcement, related developments associated with commercial genomic health and ancestry databases, and the potential impact of population wide DNA collection. The ethical analysis considers privacy and autonomy, self-incrimination, joint rights and collective responsibility.

Keywords Biometric identification · DNA identification · DNA profiling · DNA database · Genomics · Forensic genealogy · Privacy · Autonomy · Joint rights

3.1 DNA Identification

DNA can be recovered from biological material, such as skin cells or hair continuously being shed, or from bodily fluids such as blood. DNA obtained at a crime scene or collected via a cheek swab from a suspect is analysed in a laboratory to create a DNA profile. This profile can be compared with one obtained from biological material collected from a suspect or held in a DNA database. DNA identification is vital to modern criminal investigation and continues to be used with success in investigating serious crimes. While it has a strong scientific foundation, controversy

Note: Some parts of this article were previously published in
Smith, M., & Miller, S. (2021). A principled approach to cross-sector genomic data access. *Bioethics*. https://doi.org/10.1111/bioe.12919.

M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, SpringerBriefs in Ethics, https://doi.org/10.1007/978-3-030-90256-8_3

has occurred, for example due to contamination or other human errors in collection or laboratory testing, resulting in inaccuracies. DNA is a form of circumstantial evidence and is presented in a criminal trial in the context of a range of other evidence. If there was strong evidence that a defendant could not have been present at a crime scene, for example they were in another location at the time the crime was committed, and their DNA may have been innocently deposited there, it may not incriminate the defendant (Smith, 2016).

Repetitive regions of DNA within the genome, called *short tandem repeats* (STRs), exhibit variation between individuals in terms of the number of repeats present at each site. A DNA profile is created by analysing the number of STRs that occur at specific sites in an individual's genome. The STRs used in DNA identification are present in *non-coding* regions of the human genome: these regions do not code for genes and do not provide any health or other information about the individual aside from their identity. A match between two DNA profiles, such as one from a crime scene sample and one from a suspect sample, provides a strong basis for inferring that the samples are from the same person. An example of a DNA profile is the following gender designation (XY for male; XX for female) and set of paired numbers representing the number of repeats at STR sites on each strand of DNA, for example: 'XY 9,12 18,21 14,16 14,14 15,16 25,28' (Smith, 2016).

DNA identification was first used in a criminal investigation in 1987, when Professor Alec Jeffreys analysed biological samples recovered from two murder victims, and compared these with a sample of a suspect who had confessed to the crime. While it established that the suspect's DNA did not match the sample recovered from the victim, subsequent DNA screening of all the men from three surrounding villages was conducted, and Colin Pitchfork came to attention after coercing another into providing a sample on his behalf. Pitchfork's DNA profile matched one found at the crime scene, leading to his conviction (Jobling & Gill, 2004).

The collection of the biological sample is a critical step in DNA identification. If a sample has been planted at a crime scene, or is otherwise contaminated, the validity of the results can be compromised. It follows that DNA should not be interpreted in isolation of the other evidence in a criminal investigation or trial. The trial of O.J. Simpson in California in the mid-1990s highlighted that despite a firm scientific foundation, if collection procedures are not strictly followed, the value of the evidence can be compromised. In that early case, television footage of the crime scene was used by the defence to demonstrate that investigators had entered the scene without protective clothing, not worn protective gloves, and had dropped swabs on the ground prior to securing them in evidence bags, leading to the evidence being discredited (Smith, 2016).

DNA databases are collections of DNA profiles, indexed into categories, e.g. suspects, convicted offenders, crime scene profiles. A legislative definition of a DNA database is as follows:

> …a database (whether in computerised or other form and however described) containing (a) the following indexes of DNA profiles: a crime scene index, a missing persons index, an unknown deceased persons index, a serious offenders index, a volunteers index, a suspects

index, and information that may be used to identify the person from whose forensic material each DNA profile was derived; (b) a statistical index; and (c) any other index prescribed by the regulations.[1]

Millions of DNA profiles are collected and stored by law enforcement agencies to assist in the investigation of serious crimes, and the size of these holdings continue to grow each year. In 2021, the US National DNA Index System (NDIS) contains over 18.5 million profiles, the UK's National DNA Database (NDNAD) over 6.6 million profiles, and the Australian National Criminal Investigation DNA Database (NCIDD), more than 1.2 million profiles (FBI, 2021; UK Government, 2021; ACIC, 2021). Significantly, the United Kingdom's holding represents 10% of the total population.

There have been proposals to establish population wide DNA databases for law enforcement purposes (also referred to as, universal, in the sense that they could encompass a country's entire population), to improve the investigation of crime. Many would object to a national database of DNA profiles, with individuals (including children) included irrespective of whether they have been convicted of committing a crime, as an affront to their individual privacy and autonomy (Smith, 2018). However, as discussed in Chap. 2, similar databases are being established with other biometrics, such as facial recognition databases, by drawing on repositories of drivers licence and passport images. The following section considers legal developments, including prominent UK cases relating to the retention of DNA profiles from suspects that have not been convicted of a crime– a highly relevant to the potential establishment of population wide forensic databases.

3.2 Legal Issues

In the legal system, legislation and case law governs how DNA evidence can be used in law enforcement investigations and criminal trials. Forensic procedures legislation and evidence law regulates the circumstances in which forensic samples may lawfully be obtained and retained, and when evidence may be admitted at trial.[2] Provisions exist in most jurisdictions to enable evidence that has been obtained improperly, to be admitted if the desirability of admitting the evidence outweighs the undesirability of not doing so, in the context of a particular trial. Therefore, if a court considers evidence to be so important that it would be unjust for it not to be used, it may allow the use of evidence at trial even if investigators obtained it illegally. However, courts will also be concerned that the expert presenting the evidence has the appropriate knowledge, skill, experience, training, or education;

[1] Section 23YDAC of the *Crimes Act 1914* (Cth) (Australia).

[2] See, e.g. in the United States, the DNA Fingerprint Act of 2005 allows an arrestee's profile to be uploaded to the federal database at the time of arrest. If the arrestee is not subsequently charged with an offence, the burden lies with the arrestee to file a court order stating that the charges have been dismissed.

whether the evidence is based on reliable scientific principles and methods; and whether it has been tested, subjected to peer review, and is generally accepted in the scientific community.[3]

Whether a law enforcement agency can collect and retain biological samples and create DNA profiles differs by jurisdiction. Generally, criminal procedure legislation in democratic countries around the world requires that there be a reasonable suspicion that a suspect has been involved in a crime before their DNA can be taken; and that they have been convicted an offence, in order for it to be indefinitely retained in a DNA database. In the United States, the Fourth Amendment of the Constitution governs the legitimacy of government intrusion into the lives of private citizens, protecting the 'right of the people to be secure in their persons…against unreasonable searches and seizures'. In order to be considered reasonable, a search needs to be supported by a warrant on the basis of probable cause: the reasonable belief that the individual has committed a crime.

Relevant cases in the United States include *Commonwealth v Cabral*[4] where it was held that there is no violation of the Fourth Amendment when a police investigator, following a rape suspect, observed the suspect spit on the street, and collected the saliva (containing skin cells), prior to establishing a match with the sample recovered from a victim. While the suspect did have a reasonable expectation of privacy in his saliva, when he expectorated and did not retrieve it, he assumed the risk of the public witnessing the act and taking possession of it. In *Cabral*, the court relied on *Commonwealth v Ewing*[5] which found no expectation of privacy in cigarette butts that had been disposed of following a police interview. The more recent Supreme Court case *Maryland v King*[6] also addresses the issue of arrestee DNA. King was arrested on assault charges and his DNA subsequently collected and retained in the state DNA database. Before he was convicted of the assault charge, his DNA profile was found to match a crime scene sample from an unsolved rape case in 2003, and he was convicted of that offence. King argued that the DNA match should have been suppressed because the Maryland DNA collection legislation allowing the database search violated the Fourth Amendment. While the Maryland Court of Appeals found the legislation was unconstitutional, and set aside the rape conviction, the Supreme Court overturned this decision and held that the retention and searching of DNA profiles against databases is a legitimate and constitutionally valid procedure to identify arrestees and determine the level of risk they pose to the community.

A significant case involving the retention of DNA evidence in the United Kingdom and Europe is *R v Marper & S*.[7] This focused on whether the *Criminal*

[3] See e.g. in the United States, Federal Rules of Evidence, rule 702; *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

[4] 69 Mass.App.Ct. 68, 2007.

[5] 67 (Mass.App.Ct. 531, 2006).

[6] 569 US 435 (2013).

[7] (2002) EWCA Civ 1275

Justice and Police Act 2001 (UK) contravened Article 8 of the *European Convention on Human Rights* relating to individual privacy. The case related to two individuals (one a 12-year-old child) who were charged with separate offences (the theft of a bike, and a domestic violence that was later dropped). Samples were obtained and DNA profiles created and included in the national DNA database. Following their acquittal, police refused to destroy the DNA profiles. This was appealed to the House of Lords,[8] followed by the European Court of Human Rights, which delivered its decision in December 2008.[9] The Court ruled in favour of Marper and S, finding that:

> …the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard.[10]

The case did not focus on whether police had the legal right to obtain the evidence, but whether retaining it breached the right to private life of the individuals concerned, under Article 8 of the Convention, and the right to fair and equal treatment under Article 14. It highlighted what could be considered an unfair distinction between individuals suspected and charged with an offence but subsequently released without conviction; and those in the broader community who had never been suspected of committing, and never been charged with committing a criminal offence.

Following the *Marper* ruling in 2008, the United Kingdom Government responded with a number of policy changes over the following years. The DNA profiles of children younger than 10 were removed from the database and legislative amendments were announced. Individuals convicted of a recordable offence still have their DNA profiles retained indefinitely; however, under the amended legislation, the government committed to, among other measures, deleting the profiles of persons arrested but not convicted of other offences after a specified number years.

In 2020, the decision in *Marper* was reaffirmed in *Gaughran v The United Kingdom*.[11] The European Court of Human Rights, in this case, ruled that the indefinite retention of biometric data (a digital DNA profile, fingerprints, and photographs that could be used for biometric facial recognition) of an individual convicted of a relatively minor offence, was a breach of a person's right to respect for their private life under Article 8 Convention. The government had sought to retain Gaughran's biometric data indefinitely, without any reference to the degree of seriousness of the offence committed or the need for retention, and with no opportunity for review of the decision. The Court held that this approach was unnecessary, failed to strike a

[8] *R v Marper & S* (2004) UKHL 39.

[9] *Case of S. and Marper v The United Kingdom* ECtHR, 4 December 2008.

[10] Ibid, 119.

[11] *Case of Gaughran v. The United Kingdom* (Application no. 45245/15) ECtHR, 13 February 2020.

fair balance between the relevant competing public and private interests, and was a disproportionate interference with Gaughran's right to respect for his private life:

> For the reasons set out above, the Court finds that the indiscriminate nature of the powers of retention of the DNA profile, fingerprints and photograph of the applicant as person convicted of an offence, even if spent, without reference to the seriousness of the offence or the need for indefinite retention and in the absence of any real possibility of review, failed to strike a fair balance between the competing public and private interests. The Court recalls its finding that the State retained a slightly wider margin of appreciation in respect of the retention of fingerprints and photographs. However, that widened margin is not sufficient for it to conclude that the retention of such data could be proportionate in the circumstances, which include the lack of any relevant safeguards including the absence of any real review.
>
> Accordingly, the respondent State has overstepped the acceptable margin of appreciation in this regard and the retention at issue constitutes a disproportionate interference with the applicant's right to respect for private life and cannot be regarded as necessary in a democratic society. There has accordingly been a violation of Article 8 of the Convention.[12]

3.3 Genomics and Forensic Genealogy

The most recent developments in law enforcement use of DNA identification should be understood in the context of corresponding medical advancements. Since the 1990s, genomic medicine has been increasingly important in understanding and treating health conditions, particularly since the completion of the Human Genome Project, by the United States Department of Energy and the National Institutes of Health in 2003, which located and sequenced all human genes (NHGRI, 2019).

Genomics-based predictive health screening to identify predisposition to specific diseases, inform lifestyle choices and improve health outcomes, is now widely available. As is genomics-based ancestry analysis, indicative of the ethnic background or global region a person descends from. Population genome screening programs have been established in a number of countries, steps toward population-wide databases that will further expand medical knowledge and treatment (Feero et al., 2018). Benefits include new therapies and greater understanding of a populations' predisposition to specific diseases, which can inform public health interventions.

Genomic information can not only reveal details of a person's health and susceptibility to disease; but also their ethnic background, paternity and relationship to others. It is also associated with increasingly important issues relating to data security, privacy and trust; and requires ongoing development of standards and frameworks to regulate genomic data sharing (Capps et al., 2013; GALGH, 2019). The *Nuffield Council on Bioethics* has identified scientific developments in genomics, and their relationship to crime and security, as a key issue for society to address this decade (Nuffield Council on Bioethics, 2019). Previously, ethics and regulation in this area has focused on specific technologies, such as gene editing, rather than the regulation of genomic data, which is rapidly growing in importance (Gyngell &

[12] Ibid, 96–8.

Savulescu, 2015). While there are existing ethical guidelines and regulation relating to the use of genomic data in clinical practice, there are gaps that may require new approaches to consent to be developed, given that the implications of genomics extend beyond a single individual (Kaye et al., 2015).

Direct-to-consumer (DTC) genomics companies offering mail-order testing, for health diagnosis and ancestry testing, are now widely available on the internet. The largest include 23andMe and Ancestry.com, which offer increasingly accessible pricing structures as the cost of the associated technology decreases. GEDmatch allows users to upload data produced by other companies to search for potential genetic relatives. Consumers of these services receive testing equipment in the mail, undertake their own cheek swab, and return it to the company, which provides the results by email, discarding the biological material but retaining the genomic data. By 2020, more than 15 million people had submitted to Ancestry.com and more than 10 million to 23 and Me (Regalado, 2019).

In this context, cross sector use of genomic health and ancestry data by law enforcement (forensic genealogy) has arisen. If law enforcement conducting an investigation do not obtain a match for a suspect's DNA profile on their national database, and it is a significant crime that warrants the investment of further time and resources, they have, in some instances, resorted to searching the holdings of a commercial genomic database, in an attempt to identify their suspect (Phillips, 2018).

Forensic genealogy involves searching for a potential common ancestor of their suspect who is a consumer of a DTC genomic testing company. It is therefore vastly broader in scope than traditional one-to-one matching against a database of convicted offenders that occurs with searches of established DNA databases. Forensic genealogy enables searching as widely as fourth cousins of the individual donor that submitted their genomic data to a health or ancestry testing company, estimated to be, on average, approximately 100 individuals (Phillips, 2018). Given that more than 26 million people, mostly in the United States, have submitted their genomic data for testing to one of these companies, multiplying that figure by 100 provides an indication of the potential scope of the technique.

There is a detailed process that law enforcement must undertake to identify their suspect on this basis, requiring that a significant number of people be investigated and ruled out. For example, where the genetic match indicated a second cousin relationship, investigators would hypothesise a common set of great-grandparents, and use birth, death and marriage records to construct a family tree of three generations. They would then construct four family trees of the great grandparents, and narrow down the list of grandparents, parents, great uncles and aunts, uncles and aunts, siblings, first and second cousins, on the basis that, for example, some may be deceased, live overseas, or can be excluded based on other data such as age or eyewitness reports – a time consuming task that would only be justified in serious cases. Investigators would then establish a small number of individuals that would then be overtly or covertly investigated, and their DNA sought to directly compare that individual's DNA profile with the crime scene sample (Scudder et al., 2019).

Forensic genealogy is controversial in that it involves the use of genomic data not provided for the purposes of a law enforcement investigation, but by a consumer,

seeking to obtain information about their personal health and/or ancestry, who may not have anticipated its use, or capacity to be used for this purpose, nor the significant potential implications for themselves, or a member of their extended family. It is being used as a last resort to identify suspects of serious offences; however, as it lacks legislative backing and regulation, it would be particularly alarming if it became used routinely. Many genomic DTC companies do provide notice in their terms and conditions that genomic information may be used for this purpose. For example, the 23andMe privacy statement provides notice to consumers that they share information, including genomic information, with third parties, as required by 'laws, regulations, judicial or other government subpoenas, warrants, or orders'.[13]

A high profile example of evidence obtained as a result of this technique in the United States is the conviction of former police officer Joseph DeAngelo. DeAngelo was convicted of 13 murders, committed over a twelve year period in the 1970s and 1980s, and has been popularly referred to as the 'golden state killer' (Gold, 2019). Law enforcement reportedly used the GEDmatch site to identify Deangelo after identifying a distant relative of their suspect, and tracing a family tree back to the 1880s, before finally arresting DeAngelo after obtaining DNA from his rubbish and confirming a match. It has been reported that investigators have used GEDmatch in more than 100 investigations in the United States, leading to other arrests (DeLisi, 2018). Those that object to this practice argue that it amounts to a fishing expedition, rather than a targeted and proportionate law enforcement investigation, placing a large number of genetic relatives under suspicion, affecting not only to the individual that submitted their genomic data to the DTC genomics company, but potentially all their genetic relatives (Murphy, 2018).

China established a national DNA database in the early 2000s, incorporating DNA profiles from offenders and suspects in criminal investigations. However, it has recently been reported that over the past 10 years, the Chinese government began collecting DNA profiles from one-in-ten of the male general population, and in some specific areas, 100% of the population (Dirks & Leibold, 2020). China is the world leader in public surveillance, having established a social credit system incorporating a sophisticated data integration program, drawing on, among other sources, CCTV, facial recognition, metadata, financial records and automated number plate recognition (Qiang, 2019). This system detects and implements sanctions on citizens who repeatedly fail to comply with social norms.

It has been reported that in 2013, DNA profiles from all residents of the Tibetan Autonomous Region (approximately 3 million people) were collected, and in 2016, from all residents of the Xinjiang Uyghur Autonomous Region (approximately 23 million) (Dirks & Leibold, 2020).[14] In addition to identification and surveillance; analysis of the genome (DNA phenotyping) can undertaken to determine an

[13] 23andMe Privacy Policy, section 2(b)(ii), section 4(e). https://www.23andme.com/en-int/about/privacy/

[14] Other biometrics were also universally collected, including facial, fingerprint and iris templates and voice recordings.

individual's ethnicity – noting that ethnic populations within China, such as the Uyghurs have reportedly been subjected to discriminatory treatment (Qiang, 2019).

The collection of DNA profiles from 10% of males in the general population (equating to approximately 70 million men), including from preschool aged children, began in 2017 (World Bank, 2019). Using the forensic genealogy technique described above, it is possible to identify individuals from whom DNA has *not* been collected, on the basis of their genetic relatedness to individuals who have. Scientific research predicts that universal reach of a population could be achieved using this technique from a DNA database of only 2% of the total population (Scudder et al., 2019). By collecting DNA from 10% of the male population, it is likely that 100% of the Chinese population could be identified using forensic genealogy techniques.

The Chinese Government cites research of Chinese genetics, criminal investigation and missing person cases as a rationale for undertaking this DNA sampling. A translated blood collection notice issued by the Public Security Bureau in Fujian Province states:

> In order to cooperate with the foundational investigative work of the seventh national census and the third generation digital ID cards, our district's public security organs will on the basis of earlier village ancestral genealogical charts, select a representative group of men from whom to collect blood samples. This work will not only help carry on and enhance the genealogical culture of the Chinese people, but will also effectively prevent children and the elderly from going missing, assist in the speedy identification of missing people during various kinds of disasters, help police crack cases, and to the greatest extent retrieve that which is lost for the masses. This is a great undertaking that will benefit current and future generations, and we hope village residents will enthusiastically cooperate (Dirks & Leibold, 2020, 11).

The cross sector use of genomic data from health and ancestry databases for law enforcement purposes raises concerns about the adequacy of existing laws regulating forensic evidence, and overreach by investigators, particularly given the number of people that have submitted their data to these databases, and that it is likely that population wide coverage can be extrapolated, using the forensic genealogy technique. In authoritarian states such as China, the government is taking a more direct approach, obtaining genomic data from a proportion of the population that would also enable the entire population to be identified using the forensic genealogy technique, and in relation to some ethnic subpopulations, establishing universal databases. The ethical implications of these developments will be discussed in the following section.

3.4 Ethical Analysis

The expanding use of DNA/genomic data that has been described above raises a number of pressing ethical concerns. Fundamental moral principles must continue to be valued in liberal democracies, notwithstanding the benefits to individual and public health, and community safety that the unrestrained use of this data may

afford. The cross-sector use of genomic data can be understood from the perspectives of individual privacy, autonomy, public safety, and democratic accountability in various domains. These domains include law enforcement, public health, medical research, and private sector commercialization. Central to the ethical, legal and policy issues associated with genomic data is the tension that exists between the legitimate collection of information by law enforcement, health and other government agencies, as well as commercial service provision, on the one hand, and individual rights to privacy and autonomy on the other. In a criminal law and national security context, the threat of terrorism over the past 20 years has resulted in ever greater powers for law enforcement and intelligence agencies (Miller & Walsh, 2016; Miller & Gordon, 2014) to collect evidence and conduct surveillance in order to prevent, detect and disrupt these activities, and these have extended to other forms of crime (Miller, 2009).

It is sometimes assumed that the relationship between, for instance, autonomy and security is a zero-sum relationship and that, therefore, any increase in security that decreases someone's autonomy will necessarily lead to an overall loss in autonomy. This assumption is false; or, at least, it is often false. For instance, if the police have access to the DNA of all persons with a record of having committed serious crimes, then, given that the number of such persons is small but they commit a large percentage of serious crimes, their loss of autonomy in respect of control over their DNA may be more than offset not only by an overall reduction in harm, but also by an overall increase in autonomy. This is because many persons will enjoy an increase in their autonomy, namely those persons who would have been future victims of crime had the offenders in question not been incarcerated for their past crimes, or deterred from future crimes, as a result of criminal investigators' access to the DNA of these offenders. Here it is important to note that serious crimes such as grievous bodily harm, rape and domestic violence are in large part attacks on autonomy. An analogous point concerning an assumed zero-sum relationship can be made in respect of privacy and security, especially when it is taken into account that infringements of privacy can often be mitigated, such as, in the case of law enforcement's use of big-data analytics, by processes of anonymization of data prior to the point of identification of suspects. That said, increases in law enforcement powers, including increased cross-sector genomic data access, have the potential to unacceptably compromise autonomy, privacy, and other liberal democratic principles.

Public safety and security are fundamental values in liberal democracies, as in other polities, including many authoritarian ones. However, liberal democracies are also committed to democracy and individual privacy and autonomy, and, therefore, to democratic accountability (Miller & Gordon, 2014; Miller & Walsh, 2016; Miller & Blackler, 2016). Accordingly, fundamental ethical principles must continue to be valued, notwithstanding the benefits to community safety that access to commercial genomic databases, such as 23andMe or Ancestry.com, can provide by enabling law enforcement to detect and convict perpetrators of serious crimes. While debates will continue between proponents of security, on the one hand, and defenders of privacy, on the other, there is often a lack of clarity in relation to the values or principles

allegedly in conflict—these principles and the relationships between them will now be discussed.

The notion of privacy was elaborated in Chap. 2. Let us now apply that notion to the case of genomic data. First, privacy is a right that people have in relation to other persons and organizations with respect to: (a) the possession of information (including genomic data) about themselves by other persons and by organizations, for example personal health, familial and identity information stored in genomic databases; or (b) the observation/perceiving of themselves—including of their movements, relationships and so on—by other persons, for example via law enforcement having access to their genomic data that facilitates linkage with a particular location based on an analysis of biological material deposited at that site (Miller & Gordon, 2014). Genomic data is therefore implicated in both informational and observational concerns.

Second, the right to privacy delimits an informational and observational 'space', namely the private sphere (Miller & Gordon, 2014 Ch. 10; Miller & Blackler, 2016 Ch. 4). This informational space includes genomic data; specifically, the data constituting a person's genome that is particular to that person and, relatedly, a person's DNA profile. However, the right to autonomy consists of a right to decide what to think and do, and the right to control the private sphere. So the right to privacy consists of the right to exclude organizations and other individuals (the right to autonomy) from personal information, such as genomic data.

Naturally, the right to privacy is not absolute; it can be overridden (Miller & Gordon, 2014 Ch. 10; Miller & Blackler, 2016 Ch. 4; Miller & Walsh, 2016). Moreover, its precise boundaries are unclear but, arguably, person has a right that law enforcement agencies not have access to their genomic data, although this right can be overridden under certain circumstances, namely if they have been convicted of a serious crime (their DNA profile will then be included in a forensic database). For instance, this right might be overridden if an individual is reasonably expected of being involved in a crime, and police have a warrant, approval from a judicial officer, legislative authority etc., and then only for the purpose of identifying persons who have committed a specific crime. If persons have committed a serious crime, such as murder or assault, in the past, it would be morally acceptable to utilize the retention of their genomic data (*as it relates to identity, not health conditions*) by including it in a database and matching against samples obtained from crime scenes. This is a specific and targeted measure to improve public safety, and even then, the data can only be used in such a way that has been legislated for by a democratically accountable government. As discussed above, there are already millions of individuals in countries such as Australia, the U.K. and the United States included in forensic DNA databases of this type.

Third, a degree of privacy is necessary in order for people to pursue their personal projects, whatever those projects might be. Thus knowledge of someone else's health status, familial relationships or genomic identity can lead to that information and any associated vulnerabilities being exploited, or otherwise compromised. *Autonomy*—including the exercise of autonomy in the public sphere—requires a measure of privacy.

Thus far we have considered the rights of a *single* individual. However, it is important to consider the implications of the infringement, indeed violation, of the privacy of groups of people and, ultimately, of the whole citizenry by the state (and/or by other powerful institutional actors, such as corporations). Such violations on a large scale can lead to a power imbalance between the state and the citizenry and, thereby, undermine liberal democracy itself.

Accordingly, while it is morally acceptable to access genomic data for necessary circumscribed purposes, such as the provision of healthcare or medical research, or, with the consent of the relevant individuals, for ancestry testing, it would not be acceptable to collect this data in an indiscriminate manner without consent and with no legal authority, to investigate crime. However, the DNA profiles of convicted offenders on forensic DNA databases are, and arguably ought to be, available for law enforcement purposes, for example to assist in the investigation of serious crimes. The issue that then arises is the determination of the point on the spectrum at which privacy and security considerations are appropriately balanced.

In light of our notion of privacy, we are entitled to conclude that some form of it is a constitutive human good (Miller & Walsh, 2016). As such, infringements of privacy ought to be avoided. That said, as mentioned above, privacy can reasonably be overridden by security considerations under some circumstances, such as when lives are at risk. After all, the right to life is, in general, a weightier moral right than the right to privacy. Thus, utilizing genomic data in a forensic DNA database or from a suspect to investigate a serious crime such as a murder, if conducted under warrant or legislative provisions, is surely ethically justified. On the other hand, intrusive access to the genomic data of individuals, collected for another purpose, where those individuals have not had any contact with the criminal justice system, and the data was obtained without any legal authority, particularly in relation to relatively minor offences such as theft, is far less likely to be justified. Moreover, given the importance of, so to speak, the aggregate privacy of the citizenry, relatively small-scale threats to public safety are unlikely to be of sufficient weight to justify substantial infringements of privacy, for example unregulated access to the genomic relationships of millions of people by law enforcement agencies. Furthermore, regulation and associated accountability mechanisms need to be in place to ensure that, for instance, a genomic database created for a legitimate purpose, for example health or ancestry testing with the express consent of the individuals involved, is not accessed, except with the appropriate legal authority and in relation to the investigation of serious crimes.

Here we need again to stress the particular significance of genomic data but now elaborate on the reasons for this. Genomic data, and DNA profiles in particular, are (in effect, namely for our purposes here and, therefore, issues of gene-editing aside) unchanging and unalterable; therefore, they are a reliable life-long identifier. This means that they have greater utility for law enforcement than do other forms of personal data. However, it also means that there is much more at stake in terms of an individual's privacy and autonomy should this genomic data be provided to law enforcement or other agencies (including private sector ones). Moreover, the genome of a person is constitutive of that person's individual-specific (biological)

identity. Accordingly, the threshold for the infringement of an individual's right to control access to their genomic data is higher than it is for most other personal information. And there is a further point here. For the genome of a person is not only constitutive of that person's individual-specific (biological) identity, that same genome is *in part* constitutive of the individual-specific (biological) identity of the person's relatives (to a decreasing extent depending on the degree of relatedness; for example a sibling is more related than a second cousin). Accordingly, there is a species of joint right to control genomic data in play here, and not merely an exclusively individual right.

3.4.1 Joint Rights to Genomic Data

Joint rights are rights that attach to individual persons but do so jointly (Miller, 1999, 2001a Ch. 7, 2003, 2010 Ch. 2). Thus, roughly speaking, two or more agents have the right to some good if they each have a right to that good, no-one else has a right to that good, and if the individual right of one of these persons to the good is dependent on the individual rights of the others to the good. The right to control one's genome data needs to be regarded, we suggest, as a (qualified) joint right; that is, as a right jointly held with the individual's relatives. [15] If these rights are, as we are suggesting, joint rights, then it follows that an individual may not have an exclusive individual right to provide his or her genomic data to direct-to-consumer genetic testing providers, or to law enforcement. Of course, when it comes to serious crimes, the consent of an individual regarding access to his or her genomic data is not necessarily required, for example if the individual is a past offender and hence his or her genomic data in the form of a DNA profile is held in a law enforcement database. However, in cases where identifying the person who has committed a crime relies on the genomic data of relatives known to be innocent, and the relatives in question have a joint right to the data in question, then it may be that *all* of these relatives need to have consented to the collection of the genomic data in question.[16] For in voluntarily providing their DNA to law enforcement, a person is, in effect, providing law enforcement with the partially overlapping DNA data of their relatives. But presumably a person does not have a moral right to decide to provide law enforcement with another person's DNA data. Accordingly, it seems that a person, A, does not have a moral right to *unilaterally* provide law enforcement with his or her own data, namely A's DNA data, given that in doing so A is providing to law enforcement the partially overlapping DNA data of A's relatives, B, C, D etc. Rather, A, B, C, D etc. have an (admittedly qualified) joint moral right to the DNA data in

[15] It is a qualified joint right given that the genomic data of any one of the persons is not identical to the genome data of the other persons, that is, the sets of genomic data are overlapping.

[16] This consent issue adds to other problems that exist with direct-to-consumer genetic testing, such as the accuracy of the tests and the fact that the results are not provided in a clinical setting by a healthcare professional.

question, and, therefore, the right (being a joint right) has to be exercised jointly; that is, perhaps all (or most) have to agree. Naturally, as is the case with individual moral rights, joint moral rights can be overridden. For instance, A's individual right to know whether he is vulnerable to a hereditary disease might justify his providing his genomic data to health authorities and doing so without the consent of any of his relatives. Again, the joint moral right of a group of persons to refuse to provide law enforcement with the DNA data in a murder investigation, for instance, may well be overridden by their collective moral responsibility to assist the police.

3.4.2 Collective Moral Responsibility to Assist Law Enforcement

Evidently, strategies for combating crime involve a complex set of often competing, and sometimes interconnected moral considerations (e.g. some privacy rights, such as control over personal data, are as we saw above themselves aspects of autonomy); so hard choices have to be made. However, the idea of a collective responsibility on the part of individuals to jointly suffer some costs, e.g. loss of privacy rights, in favour of a collective good (prosecuting serious crime) lies at the heart of all such effective strategies (Miller, 2001a, pp. 148–150, 2010, pp. 337–8). Accordingly, we need an analysis of the appropriate notion of collective responsibility. The notion of collective responsibility in question was elaborated in Chap. 1, i.e. collective responsibility as joint responsibility (Miller, 2001a Ch. 8, 2020 Ch. 4, 2001b, 2006, 2014, 2015, 2018).

Let us now apply this concept of collective moral responsibility to access to genomic information by law enforcement agencies to investigate and prosecute crime and, in particular, to population wide DNA databases (Miller, 2018). Certainly, there is a collective good (Miller, 2003, 2010 Ch. 2) to which, let us assume, the use of this information will make a significant contribution to law enforcement, namely, the investigation and prosecution of serious crimes and the prevention of harm and preservation of the lives of those who may otherwise have been harmed if a serial killer or rapist is not brought to justice as swiftly as possible. Naturally, those whose lives would not have otherwise been preserved receive a benefit, namely, their life that those who would not have been impacted do not receive. Moreover, crime imposes economic and social costs for society that affect individuals more broadly than those who are directly victimised by crime.

As stated above, there is a collective moral responsibility of joint rights holders of DNA to provide this DNA to law enforcement, at least in the case of serious crimes. That is, their joint moral right is overridden by their collective moral responsibility. However, this collective moral responsibility applies in specific cases on a piecemeal basis; it is not a collective moral responsibility to provide their DNA data in a manner that contributes to a population wide DNA database. Moreover, it is not a collective moral responsibility to provide their DNA data on a permanent basis.

Rather they have a joint moral right that the data be destroyed upon the conclusion of the specific criminal investigation and associated trial.

3.5 Conclusion

We have described DNA identification, and the recent development of cross-sector access of genomic data, collected for health and ancestry purposes, by law enforcement for criminal investigation purposes. It is likely that these practices, which have been documented in the United States, are also being undertaken in other liberal democracies, such as Australia and the U.K., although there is not currently any publicly available data to support this. In light of these developments, we have outlined the relevant ethical principles and identified a number of actual or potential problems that arise.

The issues in this area cannot be framed in terms of a simple weighing of, let alone trade-off between, individual privacy rights versus the community's interest in public safety. The issues are far more ethically complex, and we conclude with three general points.

First, law enforcement access to and searching of the genomic data of citizens, held by private companies and created for specific purposes, without legislative oversight or regulation, and the utilization of this data in investigations, infringes privacy rights and joint moral rights to genomic data, has the potential to create a power imbalance between governments and citizens, and risks undermining important principles hitherto taken to be constitutive of the liberal democratic state, such as that an individual has the right to freedom from state interference absent prior evidence of violation by that individual of its laws, subject to transparent and appropriately justified exceptions. That said, citizens have a collective moral responsibility to assist law enforcement (assuming in doing so they are not violating the moral rights of fellow citizens).

Second, as part of the introduction of laws to regulate this activity, if these laws are deemed to be justified, the cross-sector use of genomic data in this way must be clearly and demonstrably justified in terms of efficiency and effectiveness in law enforcement investigations, and its use circumscribed accordingly, rather than by general appeal to community security or safety.

Finally, in so far as the use of genomic data created for health or ancestry purposes can be justified for the investigation of serious crimes, and privacy and other concerns mitigated, it is imperative that this use be regulation by appropriate criminal procedure legislation, and subject to accountability mechanisms to guard against misuse. Moreover, the citizenry should be aware of these applications–genomic data should only be used for specific, justified purposes, backed by legislation, and subject to judicial review.

References

Australian Criminal Intelligence Commission (ACIC). (2021). *Biometric and forensic services*. https://www.acic.gov.au/our-services/biometric-and-forensic-services

Capps, B., et al. (2013). *Imagined futures: Capturing the benefits of genome sequencing for society*. HUGO Committee on Ethics, Law and Society.

DeLisi, M. (2018). Forensic epidemiology harnessing the power of public DNA sources to capture career criminals. *Forensic Science International, 291*, 20–21.

Dirks, E., & Leibold, J. (2020). *Genomic surveillance: Inside China's DNA dragnet* (Policy Brief Report No. 34/2020). Australian Strategic Policy Institute.

Federal Bureau of Investigation. (2021). *NDIS statistics*. https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics

Feero, F., et al. (2018). Precision medicine, genome sequencing, and improved population health. *Journal of the American Medical Association, 319*, 1979–1980.

Global Alliance for Linked Genomics and Health (GALGH). (2019). *Enabling responsible linked genomic data sharing for the benefit of human health*. https://www.ga4gh.org

Gold, R. (2019). From swabs to handcuffs: How commercial DNA services can expose you to criminal charges. *California Western Law Review, 55*, 491–519.

Gyngell, C., & Savulescu, J. (2015). The medical case for gene editing. *Ethics in Biology, Engineering and Medicine, 6*, 57–66.

Jobling, M., & Gill, P. (2004). Encoded evidence: DNA in forensic analysis. *Nature Reviews Genetics, 5*, 739–751.

Kaye, J., et al. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics, 23*, 141–146.

Miller, S. (1999). Collective rights. *Public Affairs Quarterly, 1*(4), 331–346.

Miller, S. (2001a). *Social action: A teleological account*. Cambridge University Press.

Miller, S. (2001b). Collective responsibility and omissions. *Business and Professional Ethics, 20*(1), 5–24.

Miller, S. (2003). Institutions, collective goods and individual rights. *Protosociology, 18*, 184–207.

Miller, S. (2006). Collective moral responsibility: An individualist account. *Midwest Studies in Philosophy, XXX*, 176–193.

Miller, S. (2009). *Terrorism and counter-terrorism: Ethics and liberal democracy*. Blackwell.

Miller, S. (2010). *The moral foundations of social institutions: A philosophical study*. Cambridge University Press.

Miller, S. (2014). Police detectives, criminal investigations and collective responsibility. *Criminal Justice Ethics, 33*(1), 21–39.

Miller, S. (2015). Joint epistemic action and collective responsibility. *Social Epistemology, 29*(3), 280–302.

Miller, S. (2018). Joint epistemic action: Some applications. *Journal of Applied Philosophy, 35*(2), 300–318.

Miller, S. (2020). Freedom of political communication, propaganda and the role of epistemic institutions. In M. Christen, B. Gordjin, & M. Loi (Eds.), *Ethics of Cybersecurity*. Springer.

Miller, S., & Blackler, J. (2016). *Ethical issues in policing*. Routledge.

Miller, S., & Gordon, I. (2014). *Investigative ethics: Ethics for police detectives and criminal investigators* (1st Edn.). Blackwell.

Miller, S., & Walsh, P. (2016). NSA, Snowden and the ethics and accountability of intelligence gathering. In J. Galliott & J. Reed (Eds.), *Ethics and the future of spying: Technology, intelligence collection and national security* (pp. 193–204). Routledge.

Murphy, E. (2018). Law and policy oversight of familial searches in recreational genealogy databases. *Forensic Science International, 292*, 5–9.

National Human Genome Research Institute (NHGRI). (2019). *A brief guide to genomics*. https://www.genome.gov/about-genomics/fact-sheets/A-Brief-Guide-to-Genomics

Nuffield Council on Bioethics. (2019). *Horizon scanning workshops*. Retrieved from https://nuffieldbioethics.org/future-work/horizon-scanning-workshops

Phillips, C. (2018). The Golden State Killer investigation and the nascent field of forensic genealogy. *Forensic Science International: Genetics, 36*, 186–188.

Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy, 30*, 53–67.

Regalado, A. (2019, February 11). More than 26 million people have taken an at-home ancestry test. *MIT Technology Review*. https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/

Scudder, N., et al. (2019). Policy and regulatory implications of the new frontier of forensic genomics: Direct-to-consumer genetic data and genealogy records. *Current Issues in Criminal Justice, 31*, 194–216.

Smith, M. (2016). *DNA evidence in the Australian legal system*. Lexis Nexis.

Smith, M. (2018). Universal forensic DNA databases: Balancing the costs and benefits. *Alternative Law Journal, 43*(2), 131–135.

United Kingdom Government Official Statistics. (2021). *National DNA database statistics.* https://www.gov.uk/government/statistics/national-dna-database-statistics

World Bank. (2019). *Population total: China*. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=CN