Quasi-Universal Forensic DNA Databases

Miller, Seumas; Smith, Marcus

DOI
10.1080/0731129X.2022.2141021

Publication date
2022

Document Version
Final published version

Published in
Criminal Justice Ethics

Routledge
Taylor & Francis Group

Criminal Justice Ethics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcre20

Quasi-Universal Forensic DNA Databases

Seumas Miller & Marcus Smith

To cite this article: Seumas Miller & Marcus Smith (2022) Quasi-Universal Forensic DNA Databases, Criminal Justice Ethics, 41:3, 238-256, DOI: 10.1080/0731129X.2022.2141021

To link to this article: https://doi.org/10.1080/0731129X.2022.2141021

Published online: 16 Nov 2022.

Criminal Justice Ethics, 2022
Vol. 41, No. 3, 238–256, https://doi.org/10.1080/0731129X.2022.2141021

ARTICLE

Quasi-Universal Forensic DNA Databases

SEUMAS MILLER * & MARCUS SMITH **

This article considers individual rights and fundamental tenets of the criminal justice system in the context of DNA evidence, in particular recent advancements in genomics that have significantly advanced law enforcement investigative capabilities in this area. It discusses a technique known as Investigative Genetic Genealogy (IGG) which utilizes genomic data held by commercial direct-to-consumer ancestry and health companies to investigate the identity of suspects linked to serious crimes. Using this technique, even if only a small proportion of the population (e.g. 5%) has submitted genomic data to these companies, almost anyone in the population can be identified. We discuss this phenomenon in the context of the existing literature and arguments in relation to universal forensic DNA databases, as well as relevant recent developments in both liberal democracies and authoritarian states. We introduce the concept of a quasi-universal forensic DNA database and consider associated implications for the criminal justice system and society from the perspectives of privacy, the right not to self-incriminate, joint rights, and collective responsibility.

Keywords: DNA evidence, DNA databases, investigative genetic genealogy, privacy, autonomy, collective responsibility

I. Introduction

This article critically examines the ethical implications of contemporary forensic DNA identification. It considers individual rights and fundamental tenets of the criminal justice system in light of technological advancements in genomics and associated law enforcement capabilities. Specifically, it discusses universal forensic DNA databases (including the DNA profiles of all persons in a jurisdiction) and examines the implications of contemporary techniques that have made it possible to identify almost anyone

*Professor Seumas Miller holds research positions in philosophy at Charles Sturt University, the University of Oxford and Delft University of Technology.
**Marcus Smith is Associate Professor in Law, at Charles Sturt University. Email: marcussmith@csu.edu

by linking an unknown DNA profile from a crime scene to an individual through their relatives and birth registry records, if the DNA from a certain proportion of the population has been collected: a technique known as Investigative Genetic Genealogy (IGG). In jurisdictions where a sufficient proportion of the population are included in these genomic databases, law enforcement agencies can identify any unknown individual from a sample of their DNA, effectively enabling universal coverage of the population. We describe this as a quasi-universal forensic DNA database. This scenario is critically examined from the perspectives of autonomy/privacy, the right not to self-incriminate, and collective responsibility.

Section II of the article describes universal forensic DNA databases, and discusses associated arguments, debate on the subject, a short-lived database of this type that previously existed in Kuwait, and public survey results. It also describes the IGG technique, which facilitates the identification of an unknown individual in a population through their shared DNA and familial links. Section III discusses the widespread public collection of DNA profiles from the general population in China, a single-party state that places a greater emphasis on (supposed) community rights as opposed to individual rights. Section IV considers the ethical implications of quasi-universal forensic DNA databases and whether they would be appropriate in liberal democracies.

II. Universal Forensic DNA Databases

For over a decade, the prospect of universal forensic DNA databases, comprising the entire population of a country or jurisdiction, have been debated in public discourse in a number of countries, as well as in the academic literature, including in the United Kingdom prior to the *Marper* ruling in 2008.[1] The cost, and more significantly, individual rights arguments, in relation to the inclusion of individuals who have had no contact with the criminal justice system, have prevented their implementation, but there have been attempts by some governments. For example, in August 2015, Kuwait introduced a law stating that all citizens, residents and visitors must provide a biological sample and have their DNA profile retained, with a penalty of one year imprisonment for anyone who refuse to cooperate without a lawful justification.[2] The law was enacted as an anti-terrorism law in response to an attack in June 2015 at the Shiite Imam al-Sadiq mosque in Kuwait City, that killed twenty-seven people and seriously injured 227. In mid-2017, Kuwait's highest court ruled against the law on the basis that it violated liberty and privacy provisions in their Constitution.[3]

In most countries around the world, national databases of DNA profiles of convicted offenders and suspects have been established. These contain millions of profiles. For example, in the United States the National DNA Index System contains approximately thirteen million convicted offender profiles (from a

total population of 328 million);[4] the United Kingdom's National DNA Database contains about six million offender profiles (from a total population of sixty-seven million);[5] and China has established the world's largest DNA database, believed to include approximately 140 million profiles, not limited to those that have been convicted of a criminal offence, but also obtained through public collection programs (from a total population of 1.4 billion).[6]

Universal forensic DNA databases and the prospect of entire populations submitting DNA to the police or government are not a realistic scenario in the near future in liberal democracies. However, the merits of establishing universal databases have been discussed in the literature and debated in a number of countries around the world over the past fifteen years.[7] Proponents assert that universal databases would significantly enhance the investigation and prosecution of crime and are fairer than regimes that include suspects, because they treat all citizens equally.[8] Conversely, others have highlighted the considerable cost that would be associated with creating the database and argue that it is not justifiable to include individuals who have not committed a crime.[9]

Public opinion of universal databases has been assessed in surveys in a number of countries. In Portugal, a survey of the general public published in 2014 found that 46% of respondents would accept the inclusion of their DNA profile in the national database, and 23% would refuse (with approximately 30% undecided).[10] A survey undertaken in Wales published in 2010, found that 60% of participants supported a universal database. However, a New Zealand survey published in 2009 found that only 23% supported a universal database.[11] It appears that the opinions on universal databases of the general public in a number of countries around the world vary significantly.

Over the past decade, a technique known as IGG, has enhanced the scope of DNA profiling to identify suspects that are not included in traditional DNA databases. It exploits the inherited nature of DNA to facilitate the identification of an individual, even if their DNA profile is not held on a DNA database, by virtue of their genetic relatedness to a relative that purchased commercial genetic health or ancestry testing. The most prominent example of forensic genealogy to date is the "golden state killer" case in California. The offender was identified only because a distant relative had purchased commercial genetic testing and investigators were able to access the company's data repository. If a match of any significance is obtained in one of these data sets, and scientific evidence expects matches up to third cousins of suspects, the suspect could be identified using births, deaths and marriages records, and traditional police work:

> *If we suspect that the person who deposited the sample and 'B' are second cousins or share another relationship of similar genetic distance (such as first cousins twice removed) we then hypothesise that they share at least one common ancestor, most likely a set of great-grandparents. To identify suspects, it would therefore be necessary to build that family tree upwards three generations from 'B'.*
>
> *It is then necessary to build the four family trees of the great-grandparents. These family trees would then include a significant number*

of individuals, being biologically related grandparents, parents, great uncles and aunts, uncles and aunts, siblings, and first and second cousins of 'B'.[12]

Finally, using other investigative tools, it is then necessary to narrow in on potential suspects. Some individuals in those family trees may be deceased or living abroad. Some may be too close or too distant in their genetic relationship. Other available information or intelligence, such as eyewitness reports estimating the approximate age of the suspect, could narrow the pool even further. If successful, the technique will yield a small enough list of potential suspects to allow police to take further overt or covert action.[13]

As Nathan Scudder et al. report, scientific research published by Yaniv Erlich, Tal Shor, Itsik Pe'er and Shai Carmi in 2018 predicts that universal reach of a population could be achieved using this technique from a database of as little as 2% of the total population:

Identity by descent analysis has been demonstrated operationally for family relationships at least as far as third cousins, whose common ancestor would be one set of great-great-grandparents. … The number of samples required by law enforcement to cover an entire population would be relatively small. Erlich, Shor, Carmi, & Pe'er (2018, p. 4) predict that comparing a suspect's DNA to a database representing only 2% of total population size would, provided the suspect is from that general population group, almost certainly reveal a potential third cousin or closer relative.[14]

In fact, each suspect or offender could bring with them the potential to partially match against hundreds or possibly thousands of distant relatives: living or dead, local or abroad. The United Kingdom's National DNA Database contains just over six million DNA profiles (in a population of sixty-seven million people).[15] If these six million samples had been processed with high-density DNA technology—creating perhaps a few dozen terabytes of genetic data—then a very high percentage of the entire United Kingdom population would be within genealogical reach of at least one stored profile. Such a dataset would be five times the size of the percentage Erlich, Shor, Carmi, & Pe'er predict as giving universal genealogical reach for a population group.

Based on the availability of this technique and associated scientific advancement, it would not be necessary to construct a universal forensic DNA database in order to obtain universal coverage of a population for forensic identification purposes. A conservative assessment of the sample of the population needed would be 10%. It is likely that if this percentage of the total population of a jurisdiction were included in a database that investigators could access, any unknown suspect who, for example, leaves their DNA at a crime scene, could be identified via their relatives in an existing database, even if the suspect's DNA is not in a database. In this way, law enforcement can have universal coverage of a population for criminal investigation purposes, even if a universal forensic DNA database does not exist. We describe this form of population coverage as a *quasi-universal forensic database*. It should be noted that a true universal forensic DNA database could identify a specific individual in seconds, while a quasi-universal forensic database would identify a list of relatives that need to be

winnowed and investigated. For example, a suspect may be a brother or sister of a known person, but if the known person has five siblings rather than one, further work will be required. As foreshadowed in the introduction, China has recently embarked on a massive public collection program of the general population that may facilitate the capability we discuss.

III. A Quasi-Universal Forensic DNA Database

China established a national DNA database for law enforcement purposes in the early 2000s that included DNA profiles from offenders and suspects in criminal investigations. Reports suggest that since 2010 the government began collecting samples and creating DNA profiles from the general population. In most areas of the country approximately 10% of the male population has been required to provide a DNA sample.[16] The collection of biometrics in China more broadly should also be noted. China is the "world leader" in public surveillance.[17] It has established a social credit system that incorporates a sophisticated data integration program, drawing on, among other sources, CCTV, facial recognition, metadata, financial records, and automated number-plate recognition. This system has the capacity to create a detailed picture of an individual's life and enables sanctions to be imposed on citizens if they repeatedly fail to comply with social norms. DNA is one of many forms of biometric and other data that is extensively collected.

China has also embarked on a massive public collection program of the DNA of citizens living in specific regions or of a particular ethnic background, regardless of whether they had contact with the criminal justice system. In 2013, DNA profiles from the entire population of the Tibetan Autonomous Region (with a population of approximately three million people) were collected, and in 2016 from the entire population of the Xinjiang Uyghur Autonomous Region (a population of approximately twenty-three million).[18] In addition to identification and surveillance facilitated by this DNA profiling, phenotyping can be conducted to ascertain an individual's ethnicity, a notable capacity, given that ethnic populations within China, such as the Uyghurs, have been subjected to differential treatment.

Beginning in 2017, DNA profiles have been collected from 10% of the male population (715 million) across the country, a total of 71.5 million DNA profiles. This compulsory collection reportedly includes preschool-aged children.[19] This means that the Chinese government has collected DNA from 97.5 million of China's 1.4 billion citizens, approximately 7% of the population. The size of the forensic DNA database in China has been estimated to be approximately fifty million, bringing the total number of individuals who have had their DNA collected in public collection programs or in the criminal justice system to approximately 140 million, 10% of the population.

The reasons provided for obtaining samples for the purpose of genetic profiling, include research of

ancestry and health genetics, as well as use in criminal investigations and missing persons cases. An extract from a translated blood collection notice posted by the Public Security Bureau in Fujian Province, and published by Emile Dirks and James Leibold, includes the following:

> *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.*[20]

There is no doubt that the systematic collection of DNA from a national population in this manner will contribute to genealogical research and improve law enforcement and security agency capabilities. However, questions remain whether the primary purpose of the DNA collection has been communicated, and whether the scale of the approach is justified on an ethical or legal basis. China has created the world's largest DNA database, an approach criticized by human rights groups and in the western literature, which describes it as a "dragnet."[21] The criticisms relate to: (a) the legal basis for compulsorily collecting the samples from individuals who are not suspected or convicted of involvement in a crime; (b) the issue of informed consent, as individuals may be unaware when providing a sample that this may have implications for their family members; and (c) privacy considerations associated with screening for ethnicity and other phenotypic traits. We now move to a detailed analysis of the associated ethical issues.

IV. Ethical Analysis

1. Autonomy/Privacy

As noted above, universal and quasi-universal forensic DNA databases have significant implications for individual autonomy/privacy. Here autonomy/privacy is understood primarily as informational privacy and, therefore, as an aspect of individual autonomy: more specifically, the right to control one's personal information. The threat to autonomy/privacy from these databases is considerable, since they can be used or, alternatively, misused by law enforcement for identification and investigation purposes. Moreover, DNA and other genetic information is unlike, for instance, personal financial data (e.g. funds held in one's bank account) or personal communication information (e.g. who one contacts), in that it is permanent and unalterable; one can change one's bank account or phone number but one cannot change one's DNA. Therefore, they are a reliable life-long identifier. This means they have greater utility for law enforcement than other forms of personal data. However, it also means 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. (Indeed, the same genome is *in part* constitutive of the individual-specific (biological) identity of the person's relatives. We return to this complication in the following section on joint rights.) Accordingly, the threshold for the infringement of an individual's right to control access to their genomic data is higher than for most other personal information. Further, universal or quasi-universal DNA databases can be used in conjunction with other databases, including databases of fingerprints, facial images, financial information, phone metadata, and so on. Again, while the integration of all these databases with DNA databases has greater utility for law enforcement, it also potentially undermines individual autonomy/privacy to an even greater extent than is the case if all these databases are not integrated with DNA databases.

Privacy is a right[22] that people have in relation to other persons and organizations with respect in part to the possession of information about themselves by other persons and by organizations, e.g. DNA profiles and other genomic data stored in law enforcement, government, or commercial databases. DNA profiles can enable other information, such as their health status, paternity relationships, and so on, to be derived by other persons, e.g. via law enforcement analysis of biological material at a crime scene or other site that can link a person with that particular location. Importantly, privacy rights are closely associated with the more fundamental moral value of autonomy. While privacy delimits an informational (and, for that matter, an observational) "space" (i.e. the private sphere) 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) both from personal information, such as that included in DNA, and from monitoring of where they have been and who they have been with. Hence it is a right to privacy/autonomy. Moreover, some might hold that the right to privacy as an aspect of autonomy is what is most important about it. Importantly, it is the right to privacy as an aspect of individual autonomy that is typically of fundamental concern to defenders of liberal democracy.

The right to privacy is not absolute. A person does not have a right not to be casually observed (as opposed to, for instance, followed around) in a public space. Arguably, however, they do have a right for law enforcement agencies not to have access to their genomic data, albeit 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 suspected of being involved in a serious 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, in the past, it would, arguably (see below), be morally acceptable to utilize the retention of their genomic data (as it relates to identity, not health conditions), to include it in a database and match it against samples obtained from crime scenes. This is a specific and targeted measure to improve public safety that even then can only be used in such a way as has been legislated for by a democratically accountable government. As discussed above, millions of individuals in countries such as the United Kingdom and the United States have already been included in forensic DNA databases of this type since the early 2000s. However, this justification for retention of DNA profiles does not extend to innocent persons or even to suspects who are not subsequently convicted of crimes. Accordingly, it does not justify universal or quasi-universal forensic DNA databases, in so far as the latter involve the accessing of the DNA of innocent persons (e.g. those who have submitted DNA to commercial ancestry and health testing services, and their relatives), who have not consented to these DNA profiles being accessed by law enforcement.

Privacy/autonomy is a moral right of an individual. However, the implications of an infringement of the privacy/autonomy rights of groups of people and, ultimately, the citizens of an entire state, or subgroup of a state, must also be considered. Violations on a large scale can result in a power imbalance between the state and the citizenry and, thereby, undermine liberal democracy itself. The universal collection of DNA from entire populations of millions or tens of millions of people in the Tibetan Autonomous Region and the Xinjiang Uyghur Autonomous Region, for identification and analysis by the Chinese government, are striking examples of large-scale violations of privacy and autonomy rights in an authoritarian state. For one thing, as we have just seen, they violate individual autonomy/privacy rights. For another, as the social credit system in China graphically illustrates, it threatens to generate an unacceptable power imbalance between the citizenry and the state, especially when the potential to integrate DNA databases with other databases is taken into account. A cornerstone of liberal democracy is that the citizens exercise control over the state rather than the reverse.

2. Joint Moral Rights

Thus far in this article we have considered quasi-universal DNA databases in relation to individual moral rights and, in particular, the individual right to privacy/autonomy.

However, as mentioned above, the genome of a person is not only constitutive of that person's individual-specific (biological) identity, for 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, e.g. a sibling is more related than a second cousin). Evidently, therefore, genomic data involves joint rights: but what are joint rights? Roughly speaking, two or more agents have a joint moral right to some good, including potentially some data or knowledge, if they

each have an individual moral right to the good, if no-one else has a moral right to it, and if the individual right of each is dependent on the individual rights of the others. Thus, the right of moral agent A to some good, G, (jointly held with moral agent, B) brings with it an essential reference to the right of B to G (jointly held with A), and does so via the good, G. Moreover, being a joint right, neither A nor B can unilaterally waive it.[23]

Joint rights need to be distinguished from universal individual rights. Take the right to life as an example of a universal individual right. Each human being has an individual right to life. However, since my possession of the right to life is wholly dependent on properties I possess as an individual, it is not the case that my possession of the right to life is dependent on your possession of that right. Notice that joint rights can be based at least in part on properties individuals possess as individuals. The right to political participation is based in part on membership in a political community, and in part on possession of the property or right of autonomy.[24]

Joint rights can arise in a variety of ways. Joint rights can arise by way of promises. The owner of a house might confer joint ownership rights of the house on his two sons, for example. These joint rights might be joint moral rights and joint legal rights if the promise in question was legally binding. Another important moral basis for joint moral rights is joint action (of which more below); specifically, joint action which produces a good, i.e. a good to which there is a joint right. Consider, for instance, two business partners or the co-authors of a book. Again, these joint moral rights might also be joint legal rights, depending on the nature of the laws in the jurisdiction in question.

As stated above, 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. Accordingly, there is a species of joint right to control genomic data in play here, and not merely an exclusively individual right. The right to control one's genome data needs to be regarded, we suggest, as a (qualified) joint right, i.e. a right jointly held with the individual's relatives.[25] 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 consumer genetic testing providers, or to law enforcement. Of course, when it comes to serious crimes, the consent of an individual to access his or her genome data is not necessarily required, e.g. 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.[26] 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.[27] For in voluntarily providing one's DNA to law enforcement a person is, in effect, providing law enforcement with the partially overlapping DNA data of the person's 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, i.e. 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 question and, therefore, the right (being a joint right) has to be exercised jointly, i.e. perhaps all (or most) have to agree. If this is the case, then it provides an important brake on the state's ability to have recourse to quasi-universal DNA databases to bypass the objections to universal DNA databases. Naturally, as is the case with individual moral rights, joint moral rights can be overridden. For instance, A's individual's 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. In relation to our concerns here, 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. However, prior to elaborating the individual and collective moral responsibilities in play we need to discuss an important individual moral and legal right that we are yet to consider, namely the right not to self-incriminate. The moral right not to self-incriminate adds a further level of moral complexity to the issue of quasi-universal DNA databases. If members of a group with a joint moral right to DNA have a collective moral responsibility to provide samples of their DNA to law enforcement, what of that member of the group who actually committed the murder and who has, therefore, an individual moral right not to self-incriminate?

3. Right Not to Self-Incriminate

The privilege against self-incrimination entitles a person to refuse to answer any question, or produce any document, if the answer or the production would tend to incriminate that person, and is integrated into the legal systems of liberal democracies around the world, either in common law, or statute.[28] The rationale can be traced to the fact that the state has substantially more resources at their disposal in prosecuting crime in comparison with those against whom that power is exercised, and there are dire consequences such as imprisonment at stake. A further consideration is respect for the dignity and privacy of individuals.[29] It can be argued that legally requiring a person to provide DNA evidence that might inculpate themselves is a breach of the legal privilege not to self-incriminate, which is in turn based on the moral right not to self-incriminate. Let us set aside the legal privilege and focus on the apparently underlying moral right not to self-incriminate.

The right not to incriminate oneself seems to be closely related to the right to self-defence. The notion is normally held to be that no matter how heinous the crime a person may have committed they always retain the moral right to defend their life. So a convicted

murderer sentenced to death, or a terrorist sentenced to death, is morally entitled to try to prevent his or her executioner from performing the execution, even up to the last moment. Similarly, people always retain the right not to intentionally incriminate themselves, although of course they may choose to self-incriminate, just as they may choose not to defend themselves. On this view, even people who have committed a heinous crime retain the right not to, in effect, speak against themselves or otherwise intentionally facilitate their own conviction. This view is consistent with the absence of any right not to accidentally or inadvertently incriminate oneself. It is also consistent with consenting (perhaps by way of implied consent) to self-incrimination in certain circumstances, e.g. the act of driving a car might be held to imply consent to alcohol tests.

Notice that the moral right not to self-incriminate, as is the case with most, if not all, moral rights, is not absolute; so, at least in principle, it can be overridden. Of course, things might be different with the legal right not to self-incriminate, although what the legal right ought to be is a matter to be settled at least in part on moral grounds. Moreover, the moral and legal right not to self-incriminate might not apply in certain circumstances, most obviously if the person in question has already been convicted of a crime and, as a consequence, the issue of incrimination for that crime, if not for other crimes, does not arise. Further, arguably, it is morally justifiable to collect the DNA profile of a person convicted of at least some serious crimes, e.g. murder, and retain it after they have completed their sentence, on the grounds that they continue to pose such a serious risk that their right not to self-incriminate, supposing they are accused of a crime in the future, is overridden. Relatedly, it might be argued that it is morally justifiable to retain a DNA database of all those persons convicted of serious crimes on the grounds that their individual rights not to self-incriminate (now qualified as a result of their conviction) are outweighed by the contribution such a database makes to protecting the community at large. It is consistent with all these qualifications that a person, including one reasonably suspected of a serious crime, who voluntarily allows their DNA profile to be collected to enable their exculpation should have the right to have their DNA profile destroyed (perhaps after a period of time).

What of those who refuse to provide their DNA (and who have not been convicted of a serious crime)? Some of these are straightforward cases of suspects who (let us suppose) can refuse on the basis of the legal (morally based) right not to self-incriminate. Other cases are not so straightforward. Suppose there is a population or group none of whose members is a suspect in the sense of being the particular, already uniquely identified, individual suspected of the crime being investigated; rather it is merely possible or perhaps likely that one member or other of the population or group is the offender, but it is not known which one. Now suppose that most of the members of the population or group in question voluntarily provide DNA in order to assist the police and to remove any suspicion from themselves. Is

this a violation of the right not to self-incriminate of the ones who refuse to provide their DNA, given there is a joint right to the DNA in question? Of course, the exercise of a person's right to provide evidence to exculpate himself does not in such cases consist of a violation of another person's right not to self-incriminate herself. For the right of person A not to self-incriminate does not entail a duty on the part of another person, B, not to incriminate A. Moreover, if person A is to self-incriminate, then A will have to perform an action, in this scenario presumably the action of refusing to provide her DNA. Has the person who refuses to provide their DNA necessarily invoked their right not to self-incriminate? Not necessarily, given the other available moral justification for so refusing, namely, an innocent person's invocation of the exercise of their right to privacy/autonomy. However, the right to privacy/autonomy might be justifiably overridden in certain circumstances, e.g. in the case of a serial killer. Nevertheless, could the person reasonably invoke their right not to self-incriminate? Presumably they could, at least on the view of this right outlined above, but what of the matter of adverse inferences that might be drawn?

Firstly, the exercise of the right not to self-incriminate does not necessarily exclude the possibility of adverse inferences being drawn, so the protection it affords is incomplete. Secondly, if it is believed that the protection it affords should not be reduced in this way then legislation could be enacted to the effect that failure to provide DNA in these circumstances cannot be taken to constitute reasonable suspicion in a formal sense, e.g. it cannot justify arrest, let alone constitute evidence at trial. If such legislation were enacted, then the person who refused to provide her DNA would not be incriminating herself, intentionally or otherwise. (The right to silence operates in something like this manner, i.e. adverse inferences cannot be made, at least at trial.) Either way, the moral right not to self-incriminate would include the right to refuse to provide one's DNA.

Note that whereas this right to refuse to provide one's DNA in these circumstances is an impediment to criminal investigations, its effect on an investigation is mitigated if the other members of the population or group voluntarily provide their DNA and, more generally, if innocent persons discharge what might be regarded as their collective moral responsibility to provide their DNA (albeit in the context of their DNA profiles being destroyed on completion of the investigation). Let us now turn directly to the issue of collective moral responsibility.

4. Collective Moral Responsibility

As we have seen, the collection of and access to genomic information for law enforcement purposes has continued to expand over the past decade in both liberal democracies and authoritarian regimes. The public collection programs implemented in China enable all citizens to potentially be identified in a criminal investigation if necessary. This aspect of the discussion will examine whether there is *collective moral responsibility*[30] to investigate serious crime that overrides individual privacy and autonomy rights

and makes these actions morally justified.

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 favor of a collective good (prosecuting serious crime) lies at the heart of all such effective strategies. Accordingly, we need an analysis of the appropriate notion of collective responsibility.

Central to collective responsibility is the responsibility arising from joint actions and joint omissions. A joint action can be understood as follows: two or more individuals perform a joint action if each of them intentionally performs his or her individual action but does so with the (true) belief that in so doing each will do their part and they will jointly realize an end which each of them has and which each has interdependently with the others, i.e. a collective end.[31] On this view of collective responsibility as joint responsibility, collective responsibility is ascribed to individuals;[32] moreover, if the joint action in question is morally significant, e.g. by virtue of the collective end being a collective good or a collective harm, then the individuals are collectively *morally* responsible for it. Each member of the group is individually responsible for his or her own contributory action, and (at least in the case of most small-scale joint action) each is also individually (fully or partially) responsible for the aimed-at outcome, i.e. the realized collective end of the joint action. However, each is individually responsible for the realized collective end *jointly with the others*; hence the conception is relational in character. As already mentioned, if the collective end of the joint action is a collective good or a collective harm, then these individual persons are collectively morally responsible for this good or harm.

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 universal and quasi-universal DNA databases. Certainly, there is a collective good 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 be 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 victimized by crime.

Other things being equal, and assuming that a universal or quasi-universal forensic DNA database operates effectively, there is a collective moral responsibility on the part of members of the state to submit their DNA. Of course, other things might not be equal. For instance, the data made available to authorities

might be misused. Moreover, there are the moral rights to privacy/autonomy and the joint rights to DNA in play and, as we have seen, the moral right not to self-incriminate. As argued 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 universal or quasi-universal 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. And there is this further point: Someone who has a right to his DNA (albeit held jointly with his relatives) may know that he has not committed the serious crime being investigated yet not know whether he himself is a suspect by virtue of (real or imagined) evidence possessed by law enforcement. This consideration may even override his jointly held moral responsibility to provide his DNA by virtue of triggering his right not to self-incriminate (depending on how this latter notion is to be understood).

What of the moral right not to self-incriminate? Arguably, the right not to self-incriminate overrides the individual responsibility of an offender (or suspect) to provide her DNA data to law enforcement. Note that this individual moral responsibility (overridden by the right not to self-incriminate) is the offender's (or suspect's) responsibility to contribute her DNA data to assist law enforcement and, as such, is the offender's component responsibility (so to speak) of the group's collective (i.e. joint) moral responsibility to provide their DNA data to law enforcement. Accordingly, whereas most of the members of the group are, all things considered, morally required to provide their DNA data, the offender (or suspect) is not, all things considered, morally required to do so; her right not to self-incriminate, should she choose to exercise it, affords her protection at this point. However, the protection is limited in so far as law enforcement will, nevertheless, have the benefit of the DNA data of the other members of the group, and that DNA data may overlap with the offender's (if she is a relative) and, if not, an adverse inference might still be able to be made with respect to the offender (or suspect).

Notice that, as mentioned above, this conception of collective responsibility as joint responsibility implies that each relevant person has an individual moral responsibility to provide a sample of their DNA (assuming the others do). So it is not simply a matter of whether each wants to do so; rather, each has a moral obligation to comply (given the others, or most of the others, comply). However, it does not follow from this responsibility that each should be compelled to comply; it does not follow that compliance should be a matter of enforceable law. On the other hand, if the number of people who choose to comply under circumstances in which compliance is voluntary is

not sufficient to meaningfully assist the criminal investigation in question, then it may well be that compliance ought to be enforced, i.e. that the magnitude of the evil to be avoided outweighs any given individual's privacy/autonomy right and, indeed, the aggregate privacy/autonomy rights or, in the case of a group of genetic relatives, their joint moral right.

And there is this further point: Given the increasing amount of data available to public and private sector agencies, such as smartphone metadata and location history; it is important that the use of this data is only used under warrant for the investigation of serious crimes. It is important that this availability does not lead to normalization or more widespread use of sensitive data in cases where it is not appropriate.

V. Conclusion

Universal forensic DNA databases and, as we have seen, *existing* quasi-universal forensic DNA databases, compromise moral rights, notably privacy/autonomy rights, joint right to DNA, and the right not to self-incriminate. However, citizens have a collective moral responsibility to assist law enforcement in relation to serious crime and, in particular, to provide their DNA data on a case-by-case basis, if required. Indeed, this moral responsibility may need to be enforced since in relation to serious crimes it evidently overrides privacy/autonomy rights. Arguably, however, the right not to self-incriminate overrides the individual moral responsibility—including when it occurs as a component of a wider collective moral responsibility—to assist law enforcement.

In summation: First, universal forensic DNA databases should not be permitted under law if they require compelling everyone to provide DNA; this is not morally justified. Rather only the DNA of those convicted of serious crimes should be collected and retained permanently. The DNA of those arrested and charged with crimes, but not convicted, may be collected and retained for a reasonable period of time.

Second, a person reasonably suspected by law enforcement of committing a serious crime, or who is among a group of familial relatives one or more of whom is suspected of committing a serious crime, has (respectively) an individual or joint (i.e. collective) moral responsibility and ought to have a legal responsibility to provide their DNA to law enforcement for exculpatory or inculpatory purposes. Those who voluntarily provide their DNA to assist law enforcement under these circumstances and are exculpated have a moral right, and ought to have a legal right, to have their DNA destroyed within a reasonable time period, e.g. normally at the conclusion of the investigation.

Third, the individual moral and legal responsibility to provide one's DNA to law enforcement under the circumstances described above (whether or not jointly with others) is overridden by the moral right not to self-incriminate (but not by any alleged duty not to other-

incriminate) in instances where it is likely to do so. The moral right not to self-incriminate should also be a legal right. Whether or not an adverse inference should be able to be drawn at trial (and the weight to be given to such an inference) from a refusal on the part of someone charged with a serious offence to provide DNA on grounds of self-incrimination ultimately depends on the overall security threat posed by the type of crime in question.

Finally, law enforcement should not have the legal right to access DNA databases collected for other purposes, except in two sorts of case. In the first kind of case there is a particular, already uniquely identified, person who is reasonably suspected of having committed a serious crime, and access to their DNA data is granted under warrant. In the second kind of case there is a particular, already uniquely identified, person who is *not* suspected of having committed a serious crime but who is a member of a group of familial relatives one or more of whom are reasonably suspected by law enforcement of having committed a serious crime, and access to the non-suspect's DNA data is granted under warrant.

Notes

[**Disclosure Statement:** No potential conflict of interest was reported by the author(s).]

1 See e.g. Hazel et al., "Is it Time"; and Joly, Marrocco, and Dupras, "Risks." *S and Marper v United Kingdom* [2008] ECHR 1581 (*Marper*) is a significant case in the criminal justice system of the United Kingdom. The European Court of Human Rights determined that the ongoing retention of DNA profiles from individuals that have been arrested, but are later acquitted, contravenes the right to privacy provided for in the European Convention of Human Rights.

2 See Human Rights Watch, "Kuwait".

3 See Ibid.

4 See Federal Bureau of Investigation, *CODIS-NDIS Statistics*.

5 See United Kingdom Home Office, *National DNA Database Statistics;* Wiles, *Annual Report 2017.*

6 See Dirks and Leibold, "Genomic Surveillance."

7 See Smith, "Universal Forensic DNA Databases"; Smith, *DNA Evidence*; and Smith and Urbas, *Technology Law.*

8 See Kaye and Smith, "DNA Identification Databases."

9 See Loewy, "A Proposal," 261.

10 See Machado and Silva "Would You Accept," 132.

11 See Curtis, "Public Perceptions," 313.

12 Scudder et al., "Policy and Regulatory Implications," 200.

13 Ibid.

14 Ibid., 200.

15 See Wiles, *Annual Report 2017.*

16 See Dirks and Leibold, "Genomic Surveillance."

17 See Qiang, "Road to Digital Unfreedom."

18 See Dirks and Leibold, "Genomic Surveillance," 13. A range of other biometrics were also universally collected, including facial, fingerprint and iris templates, and voice recordings.

19 See World Bank, *Population Total: China*.

20 Dirks and Leibold, "Genomic Surveillance," 11.

21 A further issue that has been raised is the involvement of US biotechnology

companies in providing materials and analytical software to undertake this work, with Thermo Fisher being criticized by Human Rights Watch in 2017. The company responded that they cannot "monitor the use or application of all products that it makes": Human Rights Watch, "China: Minority Region Collects."

22 The philosophical and legal literature on privacy, including in security contexts, is vast. Some useful references include Warren and Brandeis, "Right to Privacy"; Solove, *Understanding Privacy*; Macnish, *Ethics of Surveillance*; Kleinig et al., *Security and Privacy*; Miller and Bossomaier, "Privacy, Encryption and Counter-Terrorism"; and Miller and Walsh "NSA, Snowden and Ethics."

23 For further discussion of the concept of joint rights, see Miller, "Collective Rights"; Miller, *Social Action*; and Miller, "Joint Rights."

24 Thus, the distinction between joint and collective rights or group rights is important. See e.g. Jones, *Group Rights*; and Miller, *Social Action* (Chapter 7).

25 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, i.e. the sets of genomic data are overlapping. Moreover, there is a further question with respect to the degree of overlap that would underpin a joint right. Presumably, two persons, A and B, who are very distant relatives and therefore have only have marginally overlapping genomic data might not have a joint right to the data in question; the degree of overlap is very slight and their familial relationship too tenuous to underpin a *joint* right. Accordingly, the boundaries of joint rights are vague and, as a result, fixing the limits of joint rights is somewhat arbitrary.

26 On the other hand, there is the potential collateral damage to the relatives of criminals, given partially overlapping DNA profiles.

27 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.

28 The privilege has been described in both the legal and philosophical literature: see e.g., Morgan, "Privilege against Self-Incrimination"; and Gerstein, "Privacy and Self-Incrimination."

29 See e.g., Ashworth, "Self-Incrimination"; Redmayne, "Rethinking the Privilege"; and Dennis, "Instrumental Protection."

30 For discussion of the concept of collective moral reponsibility, see e.g. Bazargan-Forward and Tollefsen, *Routledge Handbook of Collective Responsibility.*

31 For further discussion of the concept of collective ends, see Miller, "Joint Action"; Miller, "Intentions, Ends and Joint Action"; Miller, "Joint Epistemic Action"; and Miller, "Joint Action: The Individual."

32 On this point, see Miller, *Social Action* (Chapter 8); Miller, "Collective Moral Responsibility"; and Miller, "Joint Epistemic Action."

ORCID

Seumas Miller http://orcid.org/0000-0002-4851-3177
Marcus Smith http://orcid.org/0000-0001-9810-979X

Bibliography

Ashworth, Andrew. "Self-incrimination in European Human Rights Law: A Pregnant Pragmatism?" *Cardozo Law Review* 30, no. 3 (2008): 751–764.

Bazargan-Forward, Saba, and Debora Tollefsen, eds. *The Routledge Handbook of Collective Responsibility.* Abingdon: Routledge, 2020.

Curtis, Cate. "Public Perceptions and Expectations of the Forensic Use of DNA: Results of a Preliminary Study." *Bulletin of Science Technology and Society* 29, no. 4 (2009): 313–324.

Dennis, Ian. "Instrumental Protection, Human Right or Functional Necessity? Reassessing the Privilege against Self-incrimination." *Cambridge Law Journal* 54, no. 2 (1995): 342–376.

Dirks, Emile, and James Leibold. "Genomic Surveillance: Inside China's DNA Dragnet." *Policy Brief No. 34*. Canberra: Australian Strategic Policy Institute, 2020.

Federal Bureau of Investigation. *CODIS-NDIS Statistics*, 2022. http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics.

Gerstein, Robert. "Privacy and Self-Incrimination." *Ethics* 80, no. 2 (1970): 87–101.

Hazel, J. W., E. W. Clayton, B. A. Malin, and C. Slobogin. "Is it Time for a Universal Genetic Forensic Database?" *Science* 362, no. 6417 (2018): 898–900.

Human Rights Watch. "China: Minority Region Collects DNA from Millions." December 13, 2017. https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions#:~:text=(New%20York)%20%E2%80%93%20Chinese%20authorities,Human%20Rights%20Watch%20said%20today.

Human Rights Watch. "Kuwait: Court Strikes Down Draconian DNA Law." October 17, 2017. https://www.hrw.org/news/2017/10/17/kuwait-court-strikes-down-draconian-dna-law.

Joly, Y., G. Marrocco, and C. Dupras. "Risks of Compulsory Genetic Databases." *Science* 363, no. 6430 (2019): 938–940.

Jones, Peter. *Group Rights*. Farnham: Ashgate, 2009.

Kaye, David, and Michael Smith. "DNA Identification Databases: Legality, Legitimacy, and the Case for Population Wide Coverage." *Wisconsin Law Review* 2003, no. 3 (2003): 413–459.

Kleinig, John, Peter Mameli, Seumas Miller, Douglas Salane, and Adina Schwartz. *Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States*. Canberra: ANU Press, 2011.

Loewy, Arnold. "A Proposal for the Universal Collection of DNA." *Texas Technology Law Review* 48, no. 1 (2015): 261–267.

Machado, Helena, and Susana Silva. ""Would You Accept Having your DNA Profile Inserted in the National Forensic DNA Database? Why?" Results of a Questionnaire Applied in Portugal." *Forensic Science International: Genetics* 8, no. 1 (2014): 132–136.

Macnish, Kevin. *Ethics of Surveillance*. London: Routledge, 2017.

Miller, Seumas. "Collective Moral Responsibility: An Individualist Account." *Midwest Studies in Philosophy* 30 (2006): 176–193.

Miller, Seumas. "Collective Rights." *Public Affairs Quarterly* 1, no. 4 (1999): 331–346.

Miller, Seumas. "Joint Action." *Philosophical Papers* 21, no. 3 (1992): 275–299.

Miller, Seumas. "Joint Action: The Individual Strikes Back." In *Intentional Acts and Institutional Facts: Essays on John Searle's Social Ontology,* edited by S. Tsohatzidis, 73–92. Dordrecht: Springer Press, 2007.

Miller, Seumas. "Joint Epistemic Action and Collective Moral Responsibility." *Social Epistemology* 29, no. 3 (2015): 280–302.

Miller, Seumas. "Joint Epistemic Action: Some Applications." *Journal of Applied Philosophy* 35, no. 2 (2018): 300–318.

Miller, Seumas. "Joint Rights: Human Beings, Corporations and Animals." *Journal of Applied Ethics and Philosophy* 12 (2021): 1–7.

Miller, Seumas. *Social Action: A Teleological Account*. New York: Cambridge University Press, 2001.

Miller, Seumas, and Terry Bossomaier. "Privacy, Encryption and Counter-Terrorism." In *Counter-Terrorism, Ethics, and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*, edited by A. Henschke, A. Reed, S. Robbins, and S. Miller, 139–154. Dordrecht: Springer Press, 2021.

Miller, Seumas, and Patrick Walsh. "NSA, Snowden and the Ethics and Accountability of Intelligence Gathering." In *Ethics and the Future of Spying: Technology, Intelligence Collection and National Security,* edited by J. Galliott, and W. Reed, 193–204. Abingdon: Routledge, 2016.

Morgan, E. M. "The Privilege Against Self-Incrimination." *Minnesota Law Review* 34, no. 1 (1949): 1–45.

Qiang, X. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no. 1 (2019): 53–67.

Redmayne, Mike. "Rethinking the Privilege Against Self-incrimination." *Oxford Journal of Legal Studies* 27, no. 2 (2005): 209–232.

Scudder, Nathan, Dennis McNevin, Sally Kelty, Christine Funk, Simon Walsh, and James Robertson. "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, no. 2 (2019): 194–216.

Smith, Marcus. *DNA Evidence in the Australian Legal System*. Sydney: Lexis Nexis, 2016.

Smith, Marcus. "Universal Forensic DNA Databases: Balancing the Costs and Benefits." *Alternative Law Journal* 43, no. 2 (2018): 131–136.

Smith, Marcus, and Gregor Urbas. *Technology Law: Australian and International Perspectives*. Cambridge: Cambridge University Press, 2021.

Solove, Daniel. *Understanding Privacy.* Cambridge: Harvard University Press, 2008.

United Kingdom Home Office. *National DNA Database Statistics*. 2022. https://www.gov.uk/government/statistics/national-dna-database-statistics.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220.

Wiles, Paul. *Annual Report 2017: Commissioner for the Retention and Use of Biometric Material*. 2018. https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2017.

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