The retention of DNA data and the private-life interests of suspects

Bobby Naude[*]

Abstract

The mere taking of DNA samples from someone has a direct impact on his/her private-life interests. This means that, any DNA collection and retention system that permits the indiscriminate collection of DNA samples from all suspects arrested upon any charge is constitutionally unsound. There is also no acceptable justification for the indefinite retention of such samples. DNA samples should be taken from suspects and arrested persons in terms of a warrant, and such samples, and the result of any forensic DNA analysis, should be destroyed once certain conditions have been met. It is further important that a court which finds a suspect guilty, should be the same body which orders the collection of DNA samples from that person. DNA data obtained from convicted offenders should be retained indefinitely, but provision should be made for an independent body that could consider requests to have information removed from any DNA databank.

Introduction

Legislation that will set up a national DNA database for South Africa is currently in the process of becoming law. The Criminal Law (Forensic Procedures) Amendment Bill (CLFPAB)[1] *inter alia* aims to establish and to regulate the administration and maintenance of the National DNA Database of South Africa (the NDDSA).[2] The legislation will further allow certain DNA data and the information derived from such data, to be checked against the NDDSA by an authorised person.[3] This may,

* BIuris, LLD (Unisa). Professor: Department of Criminal and Procedural Law, Unisa.

1 This Bill has been introduced into the National Assembly and an explanatory summary of the Bill was published in *Government Gazette* 31759 of 29 December 2008 – see Notice 1584 of 2008. The Bill first of all inserts sections 36A, 36B and 36C into Chapter 3 of the Criminal Procedure Act 51 of 1977. The Bill also aims to substitute section 37 of the Criminal Procedure Act 51 of 1977.

2 The NDDSA is established in terms of s 15F of the South African Police Service Act 68 of 1995. (The CLFPAB inserts Chapter 5B into the South African Police Service Act).

3 See ss 36A(1)(a) of the Criminal Procedure Act 51 of 1977.

however, only be done for purposes related to the detection of crime, the investigation of an offence, or the conduct of a prosecution.[4]

The CLFPAB contains specific details about the DNA data that can be checked against the NDDSA and how this data should be obtained. In this regard, a distinction is made between the type of DNA data that can be obtained and the persons from whom it can be obtained. In terms of subsection 36B(1)(b) of the Criminal Procedure Act, a police officer must take a non-intimate sample,[5] or must cause such a sample to be taken, of any person:[6]

- arrested upon any charge;
- released on bail or on warning under section 72, if a non-intimate sample was not taken upon arrest;
- upon whom a summons has been served in respect of any offence referred to in Schedule 1 or any offence with reference to which the suspension, cancellation or endorsement of any licence or permit, or the disqualification in respect of any licence or permit, is permissible or prescribed;
- convicted by a court and sentenced to:
  – a term of imprisonment, whether suspended or not; or
  – any non-custodial sentence,
  if a non-intimate sample was not taken upon arrest;
- convicted by a court of any offence which has, by notice in the *Government Gazette*, been declared to be an offence for the purposes of the subparagraph; or
- deemed under section 57(6) to have been convicted of any offence which has, by notice in the *Government Gazette*, been declared to be an offence for the purposes of the sub-paragraph.

A police officer must immediately furnish each non-intimate sample to the National Commissioner of the South African Police Service or his or her delegate, who shall carry out a DNA analysis on each sample in terms of Chapter 5B of the South African Police Service Act,[7] and include the

---

4 *Id* at ss 36A(1)(k).

5 In terms of ss 36A(1)(I) of the Criminal Procedure Act 51 of 1977 a 'non-intimate' sample means: a sample of hair other than pubic hair; a sample taken from a nail or from under a nail; a swab taken from the mouth (buccal swab); a blood finger prick; or a combination of the aforementioned.

6 See ss 36B(1)(b) of the Criminal Procedure Act 51 of 1977.

7 Act 68 of 1995. (Chapter 5B is inserted by s 6 of the CLFPAB).

results in the NDDSA.[8] A police officer is further free to re-take a non-intimate sample from any person from whom he or she was initially allowed to take a sample, if the first non-intimate sample taken was either not suitable for DNA analysis, or if the sample proved insufficient.[9]

Non-intimate samples, or the information derived from such samples, may be the subject of a speculative search.[10] In turn, this means that the non-intimate samples – or the information derived from such samples – may, for purposes related to the detection of crime, the investigation of an offence, or the conduct of a prosecution, be checked by an authorised person against the NDDSA.[11] A non-intimate sample or the information derived from such a sample, must be retained after it has fulfilled the purpose for which it was taken or analysed, but shall only be used for purposes related to the detection of crime, the investigation of an offence, or the conduct of a prosecution.[12] Any person who uses or who allows the use of non-intimate samples or the information derived from such samples, for any purpose other than the mentioned purposes is guilty of an offence and liable on conviction to a fine or imprisonment for a period not exceeding fifteen years.[13]

The next amendment brought about by the CLFPAB, section 36C of the Criminal Procedure Act, *inter alia* deals with DNA samples for investigative purposes and further extends the number of people from whom non-intimate DNA samples can be taken. This is effected by giving a police official a discretion to take, without a warrant, non-intimate DNA

---

8 See ss 36B(2)(b) of the Criminal Procedure Act 51 of 1977.

9 See s 36B(4) of the Criminal Procedure Act 51 of 1977.

10 See s 36B(5) of the Criminal Procedure Act 51 of 1977. (Also see the proposed s 15L of the South African Police Service Act 68 of 1995).

11 See ss 36A(1)(k) of the Criminal Procedure Act 51 of 1977.

12 See ss 36B(6)(a) of the Criminal Procedure Act 51 of 1977. Section 36B(8) qualifies ss 36B(6)(a) by stating that, despite ss 36B(6)(a), non-intimate samples or the information derived from such samples shall be destroyed after five years, but only if the person is not convicted by a court of law. Also see ss 36C(3)(a) which determines that a non-intimate sample or the information derived from such a sample, must be retained after it has fulfilled the purpose for which it was taken or analysed, but shall only be used for purposes related to the detection of crime, the investigation of an offence or the conduct of the prosecution. The non-intimate samples or the information derived from such samples, which shall include, but not be limited to, the DNA profiles derived from such samples, must be stored on the NDDSA in accordance with the provisions of Chapter 5B of the South African Police Service Act 68 of 1995. Like ss 36B(6)(a), s 36C(4) states that non-intimate samples or the information derived from such samples shall be destroyed after five years if the person is not convicted by a court of law.

13 See ss 36B(6)(c) of the Criminal Procedure Act 51 of 1977. Also see ss 36C(3)(b) and ss 37(6)(b).

samples from a person, or a group of persons, if there are reasonable grounds to:

- suspect that the person, or that one or more persons in that group, has committed any offence; and
- believe that DNA samples, or the results of an examination thereof, will be of value in the investigation by excluding or including one or more of the persons as possible perpetrators of the offence.[14]

From the above it is clear that the CLFPAB not only allows for the indiscriminate taking of non-intimate DNA samples from all suspects arrested upon any charge, but in certain circumstances even from persons who are served with a summons. It appears irrelevant whether such suspects are later charged with, or even convicted of, a crime.[15] The fact that a case may be withdrawn against a specific accused, or that the accused may be found not guilty, are both immaterial to the decision of whether or not to take a non-intimate DNA sample. The Bill further provides for the indefinite retention of DNA samples, the only exception being where the accused has been found not guilty. In such an instance the samples must be destroyed after five years.[16] It is submitted that the Criminal Law (Forensic Procedures) Amendment Bill of 2008, as published, disregards the private-life interests of, especially, suspects and arrestees, and necessitates further consideration.[17] In order to appreciate the possible implications of the Bill, it is first of all necessary to have a closer look at DNA evidence.

---

14 See ss 36C(1)(a) and (b). In terms of s 36C(2), the person who has control over the DNA samples may examine them for the purpose of the investigation of the relevant offence or cause them to be so examined and may cause any non-intimate samples or the information derived from those samples to be subjected to a speculative search.

15 Section 36B(1) of the Criminal Procedure Act 51 of 1977 in fact makes it mandatory for a police official to take non-intimate DNA samples in certain circumstances.

16 See s 36B(6) of the Criminal Procedure Act 51 of 1977.

17 JC Hoeffel 'The dark side of DNA profiling: unreliable scientific evidence meets the criminal defendant' (1990) 42 *StanLRev* 465 at 533–34 captures the reason for caution: 'Imagine a society where the government had samples of tissue and fluid from the entire community on file and a computerized databank of each individual's DNA profile. Imagine then that not only law enforcement officials, but insurance companies, employers, schools, adoption agencies, and many other organizations could gain access to those files on a "need to know" basis or on a showing that access is "in the public interest." Imagine then that an individual could be turned down for jobs, insurance, adoption, health care, and other social services and benefits on the basis of information contained in her DNA profile, such as genetic disease, heritage, or someone else's subjective idea of a genetic "flaw".'

DNA data and the right to privacy

In *S and Marper v The United Kingdom*[18] the European Court of Human Rights succinctly explains the nature of DNA evidence:

> DNA stands for deoxyribonucleic acid; it is the chemical found in virtually every cell in the body and the genetic information therein, which is in the form of a code or language, determines physical characteristics and directs all the chemical processes in the body. Except for identical twins, each person's DNA is unique. DNA samples are cellular samples and any sub-samples or part samples retained from these after analysis. DNA profiles are digitised information which is stored electronically on the National DNA Database together with details of the person to whom it relates.

DNA profiles are therefore much the same as fingerprints and are used for purposes of identification. But such profiles cannot be created without DNA samples.[19] A DNA sample contains cellular information that can potentially provide detailed personal information and has serious implications as far as the right to privacy is concerned.[20]

---

[18] Applications nos 30562/04 and 30566/04. Judgment was delivered on 4 December 2008. See at note 1, par 13.

[19] See the Nuffield Council on Bioethics *The forensic use of bioinformation: ethical issues* (2007) at par 1.12 where it is explained that a DNA sample is 'the actual biological sample of body cells taken from a crime scene or from a suspect or a volunteer during an investigation'. A DNA profile, on the other hand, is a string of numbers stored on a National DNA Database. About how DNA functions as a unique identifier of individuals – see generally JD Biancamano 'Arresting DNA: The evolving nature of DNA collection statutes and their Fourth Amendment justifications' (2009) 3 *Ohio St LJ* 613; LA Matejik 'DNA sampling: privacy and police investigation in a suspect society' (2009) 61 *ArkLRev* 53 and T Maclin 'Is obtaining an arrestee's DNA a valid special needs search under the Fourth Amendment? What should (and will) the Supreme Court do?' (2006) 34 *J L Med & Ethics* 165, RC Michaelis, RG Flanders & PH Wulff *A litigator's guide to DNA* (2008). For a concise overview of the start of the forensic use of DNA – see J Parfett 'Canada's DNA databank: public safety and private costs' (2002) 29 *Man L J* 33 at 35.

[20] In *R v Chief Constable of South Yorkshire Police* [2004] UKHL 39 Baroness Hale of Richmond notes in a minority judgment (at par 71): '[T]here can be little, if anything, more private to the individual than the knowledge of his genetic make-up.' She quotes the Canadian Privacy Commissioner who, in his report on *Genetic Testing and Privacy* (1995), states: 'No surveillance technology is more threatening to privacy than that designed to unlock the information contained in human genes.' In the same report, the Canadian Privacy Commissioner also remarks (at 2): 'The measure of our privacy is the degree of control we exercise over what others know about us. No one, of course, has absolute control. As social animals, few would want total privacy. However, we are all entitled to expect enough control over what is known about us to live with dignity and to be free to experience our individuality. Our fundamental rights and freedoms – of thought, belief, expression and association – depend in part upon a meaningful measure of individual privacy. Unless we each retain the power to decide who should know our political allegiances, our sexual preferences, our confidences, our fears and aspirations,

The concern is not only an immediate one, since science may one day enable DNA analysis to reveal much more information than is currently possible, for example, behavioural traits that will show not only an individual's propensity to commit a certain type of crime, but also his or her children's propensity to do so.[21] It could also be possible to amend existing legislation to allow DNA samples to be used for purposes other than those currently stated.[22]

It is universally accepted that DNA profiles can play an important role in the detection and prevention of crime. At the same time, however, the potentially intrusive or invasive nature of the information contained in a DNA sample must be taken into account. The taking and retention of DNA samples undoubtedly infringes the right to privacy[23] and the critical

---

then the very basis of a civilised, free and democratic society could be undermined.' Also see Matejik n 19 above at 59–60 and PM Monteleoni 'DNA databases, universality, and the Fourth Amendment' (2007) 82 *NYULRev* 247 at 256.

21 The Canadian Privacy Commissioner n 20 above at 2, captures the general concern here: 'Modern explorers have set sail on voyages into the genetic microcosm, seeking a medically powerful but potentially dangerous treasure: information about how our genes make us tick. Today, we can ask who among us is likely to have healthy babies or fall ill with a genetic disease. In the future, we may be able to use genetic testing to tell us who will be smart, be anti-social, work hard, be athletic or conform to prevailing standards of beauty.' Also see the Nuffield Council n 19 above at par 6.41, and EE Joh 'Reclaiming "abandoned" DNA: The Fourth Amendment and genetic privacy' (2006) 100 *NwULRev* 857 at 876; RE Gaensslen 'Should biological evidence or DNA be retained by forensic science laboratories after profiling? No, except under narrow legislatively-stipulated conditions' (2006) 34 *J L Med & Ethics* 375.

22 See in this regard the Nuffield Council n 19 above at par 6.19 where the 'non-operational research use' of a national DNA database is discussed. Also see Joh n 21 above at 879.

23 Section 14 of the Constitution 108 of 1996 states: 'Everyone has the right to privacy, which includes the right not to have – (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed.' About the right to privacy in general, see S Woolman *et al Constitutional law of South Africa* (2ed rev serv 1 2002). In ch 38 David McQuoid-Mason points out that the concept of privacy applies to both common law and constitutional infringements of the right (at 38–21), and that in order to establish an infringement of the constitutional right to privacy, a plaintiff will have to show a subjective expectation of privacy that was objectively reasonable. In this regard the courts must strike a balance between an individual's right to privacy and the public's right to information within the norms of the Constitution. McQuoid-Mason points out that the right to privacy in s 14 of the Constitution can be broadly divided into personal autonomy cases and informational privacy cases. Because the common law has recognised variations of these two categories, it can provide useful guidelines when giving the right context. The privacy right protecting information is important for current purposes, because it 'limits the ability of people to gain, publish, disclose or use information about others without their consent'. Also see the Canadian Supreme Court's decision in *R v RC* [2005] 3 SCR 99 at pars 25–28 in this regard. About the relationship between the taking of blood tests and the right to privacy, see *Seetal v Pravitha & Another NO* 1983 (3) SA 827 (D) at 861–862; *M v R* 1989 (1) SA 416 (O) at 426–7; *Nell v Nell* 1990 (3) SA 889 (T) at 895–896; *C v Minister of Correctional Services* 1996 (4)

question is whether or how there can be any justification[24] for such an intrusion into our private lives.[25] The origin of the proposed legislation is a good place to start searching for an answer.

The position in the United Kingdom

The proposed South African legislation is to a large extent modelled on legislation applicable in England and Wales.[26] However, this legislation was discredited by the Grand Chamber of the European Court of Human

---

SA 292 (T) at 300; *D v K* 1997 (2) BCLR 209 (N). In *S v R* 2000 (1) SACR 33 (W), Willis J notes (at 39): 'There can be no doubt that blood tests entail an invasion of a person's right to privacy. In the case of *Seetal v Pravitha* ... Didcott J held that in the case of an adult an involuntary blood test unquestionably constitutes an invasion of privacy. He added, however, that the privacy of the individual is not in our law absolutely inviolable and that it may, on occasion, have to yield to other considerations of legal policy. Similarly in the case of *D v K* 1997 (2) BCLR 209 (N) it was held that an involuntary blood test constitutes an invasion of privacy. I also do not require much persuasion to accept that a blood test entails some invasion to a person's bodily integrity and security, although such invasion is slight indeed.' See also *S v Orrie* 2004 (1) SACR 162 (C) at pars 14 and 20 and the Nuffield Council n 19 above at par 3.6.

24 The justification clause in the Constitution 108 of 1996 states: '36(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including – (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose. (2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.' About the limitation of the right to informational privacy in general – see *Bernstein v Bester NO* 1996 (2) SA 751 (CC).

25 Although the current discussion will focus on privacy issues, other values concerned include liberty, autonomy and equality. A full discussion of these values is beyond the scope of this article, but see generally the Nuffield Council n 19 above at ch 3. For the reason why the privilege against self-incrimination in s 12 of the Constitution 108 of 1996 does not apply to procedures relating to the taking of blood samples, see the remarks made by Claasen J in *S v Huma* (1) 1996 (1) SA 232 (W) at 239. Also see *Levack v Regional Magistrate, Wynberg* 2003 (1) SACR 187 (SCA) at par 17 etc where Cameron JA states that 'autopic evidence', or evidence derived from an accused's own bodily features, does not infringe the right to silence or the right not to be compelled to give evidence.

26 See s 64 of the Police and Criminal Evidence Act of 1984 (as amended by s 82 of the Criminal Justice and Police Act of 2001). The Police and Criminal Evidence Order of Northern Ireland of 1989 currently governs the retention of fingerprint and DNA data in Northern Ireland and contains similar stipulations to those in force in England and Wales. In Scotland, however, the 1995 Criminal Procedure Act of Scotland stipulates that DNA samples and their resulting profiles must be destroyed if an individual is not convicted or is granted an absolute discharge. Biological samples and profiles may be retained for three years if the arrestee is suspected of certain sexual or violent offences, even if the person is not convicted – see s 83 of the 2006 Act, adding s 18A to the 1995 Act. After this, samples and information must be destroyed unless a chief constable applies to a sheriff for a two-year extension.

Rights (ECHR) in *S and Marper v The United Kingdom*.[27] In this case the court found , *inter alia,* that the retention of DNA profiles and cellular samples of the applicants was unjustified under article 8 of the European Convention of Human Rights (ECHR). Briefly, the facts were that the applicants complained that the authorities had continued to retain their fingerprints, DNA samples, and DNA profiles after the criminal proceedings against them had ended in an acquittal or had been discontinued. The first applicant was arrested at the age of eleven and charged with attempted robbery. His fingerprints and DNA samples were taken, but he was later acquitted. The second applicant was arrested and charged with harassment of his partner. His fingerprints and DNA samples were also taken, but he and his partner reconciled and the charge was dropped. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused. The applicants consequently applied for judicial review of the police decision. The Administrative Court rejected the application and subsequent appeals to the Court of Appeal and the House of Lords were equally unsuccessful.

The applicants were of the opinion that the retention of their fingerprints, cellular samples, and DNA profiles in terms of section 64 (1A) of the Police and Criminal Evidence Act of 1984, violated article 8 of the ECHR.[28] The court firstly considered whether such retention constituted an interference in the applicants' private lives. The court acknowledged that the concept of 'private life' is a broad term that is not easily confined;[29] it encompasses both the physical and psychological integrity of a person and involves multiple aspects of his/her physical and social identity.[30] Gender identification, name, sexual orientation and sexual

---

[27] Note 18 above.

[28] The relevant part of art 8 states: '1. Everyone has the right to respect for his private and family life, his home and his correspondence.' This is qualified by article 8(2) which states: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

[29] At par 66.

[30] See *Wood v Commissioner for the Metropolis* [2009] EWCA Cir 414 at par 20 where the Court of Appeal for England and Wales is of the opinion that expressions such as 'physical and psychological integrity' and 'physical and social identity' reflect the essence of the right to private life and describes it as the personal autonomy of every individual – with reference to Sir Anthony Clarke MR, in *Murray v Big Pictures (UK) Ltd* [2008] EWCA Cir 446, referring at par 31 to Lord Hoffmann's emphasis, at par 51 of *Campbell v MGN Ltd* [2004] 2 AC 457, upon the fact that 'the law now focuses upon the protection of human autonomy and dignity – "the right to control the dissemination of information about one's private life and the right to the esteem and respect of other

lifestyle are included in the personal sphere protected by article 8. So is information about a person health and ethnic identity. Article 8 also includes a right to personal development, as well as the right to establish and develop relationships with other people and the outside world. The concept of private life further includes elements relating to a person's right to his/her/their image. The court felt that the mere storing of information relating to the private life of an individual amounted to a contravention of article 8 and that the subsequent use of the stored information had no bearing on such a finding.[31]

The court noted that all three categories of the personal information retained in the case at hand, namely fingerprints, DNA profiles and cellular samples, constituted personal data.[32] It pointed out that DNA samples and profiles should be treated differently to fingerprints, since there is a larger potential for future use of the personal information they contain.[33] The court referred to the case of *Van der Velden v The Netherlands*[34] where the European Court of Human Rights held that because of the potential use to which DNA samples, in particular, could be put, their systematic retention was sufficiently intrusive to interfere with the right to respect for private life. The court held that concerns about the possible future use of personal information were legitimate and relevant to a determination of whether there had been a contravention of article 8.[35]

The court continued by pointing out that not only are DNA samples by nature very personal, but they also contain a considerable amount of sensitive information about an individual, for example, his/her health.[36]

---

people".' For a recent case that deals with the concept of 'private life' in the context of DNA evidence – see the decision by the House of Lords in *In re Attorney Generals Reference (No 3 of 1999)* [2009] UKHL 34.

31 At par 67. The court, however, points out:'I]n determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ... .'

32 At par 68. For current purposes only the court's reasoning as far as DNA profiles and cellular samples will be considered.

33 At par 69.

34 Appeal no 29514/05, ECHR (2006).

35 At par 71. The court notes: 'Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.'

36 At par 72.

DNA samples further contain an unique genetic code which is of great relevance to both the individual and his/her relatives. In view of the nature and amount of personal information contained in DNA samples, the court felt that their retention *per se* should be regarded as interfering with the right to respect for the private lives of the individuals concerned.[37] The court noted that the fact that only a limited part of the information produced by DNA profiling is actually used by the state, and causes no immediate detriment in a specific case, does not alter this conclusion. Although DNA profiles contain less information than DNA samples, profiles nonetheless contain substantial amounts of personal data. It pointed out that the use of automation to process the data enables the state to go well beyond neutral identification.[38] DNA profiles could be extended to familial searching in order to identify a possible genetic relationship between individuals.[39] This possibility is in itself enough to conclude that to retain DNA profiles interferes with the right to a private life of the persons concerned.

The processing of DNA profiles also allows the authorities to assess the likely ethnic origin of the donor.[40] This makes the retention of DNA

---

[37] At par 73.

[38] At par 75. It is, for example, possible for DNA testing to reveal rare individuals whose chromosomal sex does not match their physical sex or social gender – see the Nuffield Council n 19 above at par 2.20.

[39] The Nuffield Council n 19 above at par 2.15 explains in this regard: 'In difficult criminal investigations where a suspect cannot be identified, the police may request that "near misses" – where there may "nearly" be a match between DNA profiles – are further explored. If a crime scene profile does not completely match any subject profile on the NDNAD, it is possible to see if any subject profile could be from a relative of the person who deposited the crime scene sample. Familial searching is the process of comparing a DNA profile from a crime scene with subject profiles stored on the NDNAD, and prioritising them in terms of "closeness" to a match.' One of the risks here is that such searching might reveal unknown biological relations, or the absence of relations where they are presumed – see the Nuffield Council n 19 above at pars 6.6 – 6.12. Also see LA Hogan 'Fourth Amendment – guilt by relation: If your brother is convicted of a crime, you too may do time' (2008) 30 *WnewEngLRev* 543; DJ Grimm 'The demographics of genetic surveillance: familial DNA testing and the Hispanic community' (2007) 107 *ColumLRev* 1164; E Haimes 'Social and ethical issues in the use of familial searching in forensic investigations: insights from family and kinship studies' (2006) 34 *J L Med & Ethics* 263.

[40] At par 76. The court points out that this conclusion is consistent with the principle laid down in the Council of Europe Convention of 1981 for the protection of individuals with regard to the automatic processing of personal data ('the Data Protection Convention') and reflected in the Data Protection Act of 1998. Both these instruments list personal data revealing ethnic origin among the special categories of sensitive data attracting a heightened level of protection. Article 6 of the Data Protection Convention states that: 'Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards.' In terms of the Data

profiles all the more sensitive and heightens the effect on the right to private life.[41] The court concluded that the retention of both DNA samples and DNA profiles constitutes interference with the applicants' right to respect for their private life within the meaning of article 8 of the ECHR.[42]

The court next considered whether there can be any justification for the infringement in terms of article 8(2) of the ECHR.[43] It pointed out that section 64 of the Police and Criminal Evidence Act of 1984 is imprecise as far as the conditions attached to and arrangements for the storing and use of personal information are concerned.[44] It is widely accepted that retained samples must not be used by any person unless for purposes related to the prevention or detection of crime, the investigation of any offence, or the conduct of a prosecution.[45] The court noted that the first of these purposes is stated in general terms and may give rise to an extensive interpretation.[46]

Protection Act of 1998, 'personal data' means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (section 1). "Sensitive personal data" means personal data consisting, *inter alia*, of information as to the racial or ethnic origin of the data subject, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. (Also see Joh n 21 above at 877 in this regard).

41 The issue of equality is relevant here. In this regard the Nuffield Council n 19 above at par 3.14 points out that: 'The possibility of intensified surveillance of those individuals whose profiles are retained on forensic databases, as potential suspects, leads to the possibility of increased social exclusion of certain groups, such as young males and black minorities, who are disproportionately represented on the NDNAD ... Police powers to take and retain biological samples and the resulting DNA profiles may aggravate social tensions by discriminating against those who live in police "hot-spots" or belong to groups more likely than others to be targeted by police.' (See further at pars 3.15–3.16; pars 4.63–4.66 and par 6.12).

42 At par 77.

43 At par 87.

44 At par 98.

45 Compare ss 36A(1)(k) and ss 36B(6)(a) of the Criminal Procedure Act 51 of 1977.

46 The court states (at par 99):'It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness ...'.

The mentioned issues are, however, closely related to the broader issue of whether the interference was necessary in a democratic society. The court pointed out that the retention of personal information in this way pursues the legitimate purpose of the detection, and, therefore, the prevention of crime. The original taking of such information is aimed at linking a particular person to a particular crime. However, its retention pursues the broader purpose of assisting in the identification of future or repeat offenders.[47] The court pointed out that interference with a right will be necessary in a democratic society for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and the justifications adduced by the national authorities are 'relevant and sufficient'.[48]

A number of factors are important here; including the nature of the relevant right, its importance for the individual, the nature of the interference, and the object pursued by the interference. An important question is whether the right at issue is essential for the individual's effective enjoyment of intimate or key rights. Where a specific and important aspect of an individual's existence or identity is at stake, an infringement will not easily be justified.[49] The court held that the protection of personal data is of fundamental importance to a person's enjoyment of his/her right to respect for private life, and that 'appropriate safeguards' are essential to prevent inappropriate use of personal data.[50] It pointed out that such safeguards are particularly important where personal data undergoes automatic processing, especially where such data are used for police purposes. Such data must be relevant and not excessive in relation to the purposes for which it is stored. It must therefore be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which the data is stored.[51]

---

[47] At par 100.
[48] At par 101.
[49] At par 102.
[50] At par 103.
[51] In this regard the court refers to article 5 of the Data Protection Convention of 1981 and the preamble thereto. Article 5 deals with the quality of data and states: 'Personal data undergoing automatic processing shall be: ... b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purpose for which they are stored; ... e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.' Also see the Data Protection Act of 1998 in this regard.

It is further important that retained data be efficiently protected against misuse and abuse.[52] This is especially important in the case of DNA information which contains a person's genetic make-up. The court concludes:[53]

> The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned... .

The court then applied the stated principles to the facts of the case at hand and pointed out that no one can deny the importance of the use of modern scientific techniques of investigation and identification in the fight against crime.[54] The issue in the case at hand, however, was not a general one, but rather whether the retention of the personal information of the applicants, who had been suspected but not convicted, of certain offences, was justified.

The court pointed out that the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage.[55] With reference to DNA samples, the majority of contracting states allow such material to be taken in criminal cases only from individuals suspected of having committed offences of a 'minimum gravity'.[56] In addition, DNA samples and profiles derived from such samples are required to be removed or destroyed either immediately or within a specified limited time after

---

52 With reference to the misuse or abuse of data, art 7 of the Data Protection Convention of 1981, which deals with data security, states: 'Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.'

53 At par 104.

54 At par 105.

55 At par 107.

56 See at pars 45–49 where the court gives an overview of the law and practice regarding DNA retention in the Council of Europe member states. Also see the Nuffield Council n 19 above at box 4.3 for collection and retention powers in some European Countries.

acquittal or discharge, and only a restricted number of exceptions are allowed.[57]

The court observed that the use of modern scientific techniques in the criminal-justice system cannot be allowed at any cost, and that a careful balancing of the potential benefits of the extensive use of such techniques against private-life interests is required. The court then considered whether the retention of personal information of all unconvicted suspects is based on relevant and sufficient reasons.[58] It was willing to accept that the extension of the database in England and Wales has contributed to the detection and prevention of crime,[59] but that the question remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

The court was struck by the blanket and indiscriminate nature of the power of retention the relevant legislation provides. It noted that samples may be retained, irrespective of the nature or gravity of the offence of which a person was originally suspected, or of the age of the offender.[60] Such retention is further not time-limited, but may be retained indefinitely, whatever the nature or seriousness of the offence of which the person was suspected. A further problematic aspect is the fact that only limited possibilities exist for an acquitted individual to have DNA data removed from the nationwide database, or to have the material

---

[57] At par 108. The court refers to the position in Scotland where the retention of the DNA of unconvicted persons is only allowed in the case of adults charged with violent or sexual offences and even then, only for three years, with the possibility of an extension to store the DNA sample and data for a further two years with consent of a sheriff. The court notes that England, Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow the indefinite retention of DNA material of any person of any age suspected of any recordable offence.

[58] At par 114.

[59] At par 117. In this regard the Nuffield Council n 19 above at pars 4.47–4.52 points out that the evidence used in support of the retention regime in England and Wales is seriously limited and confusing: 'There is very limited evidence indeed that the retention regime of England and Wales is effective in significantly improving detection rates, above and beyond that which may be achieved by retaining only those profiles taken from individuals convicted of a recordable offence (as is the case in Scotland), or by simply searching against stored profiles, but not retaining the DNA profile indefinitely. The match rates between stored subject profiles and new crime scene profiles loaded onto the NDNAD in England and Wales, which is 52 per cent, can be contrasted with that of the Scottish DNA Database, which has a higher match rate of 68 per cent. This demonstrates clearly that the more limited retention policy in Scotland does not necessarily negatively impact upon its subsequent match rates (see paragraph 4.28).'

[60] At par 119. Also see the Nuffield Council n 19 above at par 4.67 in this regard.

destroyed. More specifically, there is no provision for independent review of the justification for the retention in accordance with defined criteria.[61]

The court pointed out that the state contended that retention had no significant effect on the applicants unless matches in the database were to implicate them in the commission of offences on a future occasion.[62] It, however, rejected this argument and reiterated that the mere retention and storing of personal data by public authorities, however obtained, has a direct impact on the private-life interests of the individual concerned, irrespective of whether subsequent use is made of the data.[63]

The court further noted the risk of stigmatisation as another important consideration. Although the applicants had not been convicted of any offence and were entitled to the presumption of innocence, they were treated in the same way as a convicted person.[64]

The court also emphasised that retention of unconvicted persons' data may be especially harmful in the case of minors, in view of their special situation and the importance of their development and integration in society. Particular attention should therefore be given to the protection of juveniles from any detriment that may result from retention following an acquittal.[65] Current policies, the court noted, have led to the over-

---

61 Relevant factors here would include the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances – see at par 119.

62 At par 121.

63 Also see the Nuffield Council n 19 above at pars 3.24–3.26 where it is explained why the 'no reason to fear if you are innocent' argument is unconvincing. It notes: 'First, if innocent, simply being the subject of a criminal investigation by the police can cause harm, distress and stigma. For example, if a person is one of a number of persons investigated in connection with a rape because his DNA profile matches a partial profile of the perpetrator, he may well be harmed by the taint of suspicion, both personally and socially, even if he is never arrested or charged ... Second, there are reasons to believe that erroneous implications concerning "criminality" may be drawn from the mere fact that a person's profile is on the NDNAD, even if inclusion signifies only that they have once been arrested. Indeed, the explicit justification for the extent of the Database is precisely that it is intended to represent the actual or likely criminal community ... There is thus little doubt that it is not irrational for a person to object to the retention of their biological sample and DNA profile on the Database if they have never committed a criminal act in their whole life nor will never do so.'

64 The court remarks (at par 122): 'It is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed.'

65 At par 124.

representation in the database of young persons and ethnic minorities who have not been convicted of any offence. In conclusion the court found that:[66]

> [T]he 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. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.

It is submitted that the court's finding is correct and that it captures the central issues that need to be considered before DNA samples can be taken from an individual. It is, therefore, first of all essential that DNA samples only be taken from individuals who have committed crimes of a specific gravity and with account being had to the age of the offender.[67] Secondly, it is important to place a proper time-limit on the retention of DNA samples and profiles. As a general rule, DNA samples and profiles derived from such samples should be destroyed either immediately or within a limited time after acquittal or discharge.[68] Only a restricted number of exceptions can be allowed in this regard with due consideration of the seriousness of the offence and the age of the offender. The same goes for uncharged suspects from whom DNA samples have been obtained. Thirdly, provision should be made for the independent review of any decision to retain DNA data. In this regard the seriousness of the offence, any previous arrests, and the strength of the suspicion against the person will all be important factors to consider in deciding whether DNA

---

66 At par 125.

67 Compare the Nuffield Council n 19 above at par 4.17: 'We recommend that the list of recordable offences for which fingerprints and biological samples be taken from arrestees should be rationalised so as to exclude all minor, non-imprisonable offences.'

68 As a general rule, the retention of profiles and samples can be justified as proportionate only for those who have been convicted – compare the findings by the Nuffield Council n 19 above at par 4.54.

samples and profiles should be destroyed.[69] It is necessary to compare the court's findings with legislation further afield.

The position in Canada

In Canada DNA samples are obtained in terms of a warrant,[70] once an authorisation has been obtained,[71] and when a court order to this effect has been issued.[72] A court order is the primary way by which DNA samples are obtained. In this regard section 487.051(1) stipulates that a court must make an order authorising the taking of samples of bodily substances reasonably required for forensic DNA analysis, from a person who has been convicted, discharged or found guilty under the Youth Criminal Justice Act of 2002 or the Young Offenders Act of 1985, of an offence committed at any time, provided that the offence is a primary designated offence within the meaning of paragraph (a) of the definition of a 'primary designated offence' when that person is sentenced or discharged. In this regard the court has no discretion and must make a DNA Data Bank order.[73]

The court is, however, not required to make the order if the offence is a primary designated offence within the meaning of any of paragraphs (a.1) to (d) of the definition 'primary designated offence',[74] if it is satisfied that the person has established that the impact of such an order on their

---

[69] The Nuffield Council n 19 above at par 7.37 recommends in this regard that if records are not automatically removed for those not convicted, there should be public guidelines explaining how to apply to have records removed from police databases, and the grounds on which removal can be requested. The police should further be required to justify the need for retention in response to a request for removal (with a presumption in favour of removal in the case of minors). An independent body should further oversee requests from individuals to have their profiles removed from bio-information databases. The tribunal would have to balance the rights of an individual against such factors as the seriousness of the offence, previous arrests, the outcome of the arrest, the likelihood of this individual re-offending, the danger to the public and any other special circumstances.

[70] See ss 487.05(1) and 487.05(2) of the Canadian Criminal Code of 1985. It is important to note that s 487.09(1) contains certain stipulations as far as the destruction of DNA samples obtained in execution of a warrant is concerned.

[71] See ss 487.055 and 487.091 of the Canadian Criminal Code of 1985. In *R v Rodgers* [2006] 1 SCR 554 the Supreme Court of Canada decided that the collection of DNA samples for data bank purposes from designated classes of convicted offenders is reasonable. At par 5 Charron J remarks: 'As convicted offenders still under sentence, the persons targeted by s 487.055 have a much reduced expectation of privacy. Further, by reason of their crimes, they have lost any reasonable expectation that their identity will remain secret from law enforcement authorities.'

[72] See s 487.051 of the Canadian Criminal Code of 1985.

[73] Paragraph (a) of s 487.04 lists 16 offences which are seen as the most serious and includes murder, sexual assault with a weapon, kidnapping and robbery.

[74] Paragraphs (a.1)–(d) list crimes such as hijacking, piratical acts and sexual offences.

privacy and the security of their person would be grossly disproportionate to the public interest in the protection of society and the proper administration of justice, 'to be achieved through the early detection, arrest and conviction of offenders'.[75]

Section 487.051(3) further states that a court may, on application by the prosecutor and if it is satisfied that it is in the best interest of justice to do so, make an order in relation to a person who is found not criminally responsible on account of mental disorder if that offence is a designated offence when the finding is made,[76] or a person who is convicted, discharged or found guilty under the Youth Criminal Justice Act of 2002 or the Young Offenders Act of 1985, of an offence committed at any time, if that offence is a secondary designated offence when the person is sentenced or discharged.[77] In deciding whether to make the order, the court must consider the person's criminal record, whether he or she has previously been found not criminally responsible on account of mental disorder for a designated offence, the nature of the offence, the circumstances surrounding its commission and the impact such an order would have on the person's privacy and the security of their person and must give reasons for its decision.

When an offender is convicted of a secondary designated offence, the burden is on the prosecution to show that an order would be in the best interests of the administration of justice.[78] In the case of a primary designated offence, a DNA order must be made unless the judge is satisfied that the offender has established that section 487.051(2) should apply instead.[79] In the case of primary designated offences, it can be said

75 See s 487.051(2).

76 See ss 487.051(3)(a).

77 See ss 487.051(3)(b). Secondary designated offences include crimes such as assault, intimidation, indecent acts and drug related offences.

78 Compare *R v SAC* [2008] 2 SCR 675 at pars 42–43.

79 Compare the remarks made by the Supreme Court of Canada in *R v RC* (n 23 above at par 20. Fish J, for the majority, comments: 'Much like the provision at issue in *R. v. Araujo*, [2000] 2 S.C.R. 992 ... s.487.051(2) can be described as a "constitutional compromise" that seeks to strike an appropriate balance between individual rights and societal interests. In applying this provision, court must determine whether a DNA order would adversely affect the individual's privacy and security interests in a manner that is grossly disproportionate to the public interest ... s. 487.051(2) implies that the public interest in a DNA order lies in the protection of society through the early detection, arrest and conviction of offenders ... Other objectives include deterring potential repeat offenders, detecting serial offenders, streamlining investigations, solving "cold cases", and protecting the innocent by eliminating suspects and exonerating the wrongly convicted ... .'

that the public interest is 'presumed to outweigh' privacy interests, but section 487.051(2) recognises that this is a rebuttable presumption.[80]

In considering a DNA order, a court must weigh the competing interests to ensure that the privacy and security of a person are not affected in a 'grossly disproportionate' manner. This must be done in a contextual manner, by taking the seriousness of the offence, the particular circumstances of the offence, and the character and profile of the offender into account.[81]

Section 487.053 of the Canadian Criminal Code of 1985 specifically states that a court may make an order authorising the taking of DNA samples when it imposes a sentence on a person, finds the person not criminally responsible, or directs that the person be discharged.

In Canada, DNA samples are taken up in a national DNA data bank that consists of a crime scene index and a convicted offenders index, The samples are used for criminal investigation purposes.[82] Access to information in the crime scene index shall be permanently removed if the information relates to a DNA profile derived from a bodily substance of a victim of a designated offence that was the object of the relevant investigation, or if a person has been eliminated as a suspect in the relevant investigation.[83] Information on the convicted offenders index must be kept indefinitely, but must be permanently removed after every

---

[80] Compare *R v RC* n 23 above at par 24.

[81] Compare the remarks made by Fish J in *R v RC* n 23 above at par 29. He notes (at pars 30–31): 'Some of the factors that may be relevant to this inquiry are set out in s. 487.051(3): the criminal record of the offender, the nature of the offence and the circumstances surrounding its commission, and the impact such an order would have on the offender's privacy and security of the person ... This is by no means an exhaustive list. The inquiry is necessarily individualized and the trial judge must consider all the circumstances of the cases. What is required is that the offender show that the public interest is clearly and substantially outweighed by the individual's privacy and security interests.'

[82] See s 5(1) of the DNA Identification Act of 1998. In terms of s 5(3) the crime scene index must contain DNA profiles derived from bodily substances that are found: '*(a)* at any place where a designated offence was committed; *(b)* on or within the body of the victim of a designated offence; *(c)* on anything worn or carried by the victim at the time when a designated offence was committed; or *(d)* on or within the body of any person or thing or at any place associated with the commission of a designated offence'. The convicted offenders index shall contain DNA profiles derived from bodily substances that are taken under orders and authorisations in terms of the DNA Identification Act of 1998 in compliance with the Criminal Code of Canada and the National Defence Act of 1985 – see s 5(4).

[83] See s 8.1 of the DNA Identification Act of 1998.

order or authorisation for the collection of bodily substances from a specific person has been set aside; after the person has been finally acquitted of every designated offence in connection with which an order was made or an authorisation was granted; or one year after the day on which the person has been discharged absolutely, or three years after the day on which he or she has been discharged conditionally, of a designated offence if they are not subject to an order or authorisation that relates to another designated offence, and are neither convicted of, nor found not criminally responsible on account of mental disorder for, a designated offence during that period.[84]

The position in the USA

In the USA, DNA samples are collected in terms of both federal and state laws. While federal law provides a structure and enables the sharing of DNA profiles between the states,[85] the states themselves determine whose DNA can be collected and retained.[86]

In terms of the DNA Fingerprint Act of 2005,[87] the FBI can *inter alia* retain the DNA identification record of:

- persons convicted of crimes;
- persons who have been charged in an indictment with a crime; and
- other persons whose DNA samples are collected under applicable legal authorities, provided that DNA samples that are voluntarily submitted solely for elimination purposes shall not be included in the National DNA Index System.[88]

The DNA Analysis Backlog Elimination Act of 2000 further permits the Attorney-General to collect DNA samples from individuals who are

84 See ss 9(1)–9(2) of the DNA Identification Act of 1998. In terms of s 9.1(1), access to information in the convicted offenders index in relation to a young person who has been found guilty under the Young Offenders Act of 1985 or under the Youth Criminal Justice Act of 2002 of a designated offence shall be permanently removed without delay when the record relating to the same offence is required to be destroyed, sealed or transmitted to the National Archivist of Canada.

85 This happens through the federal database which is known as CODIS (Combined DNA Index System), and it serves as a link between the databases of each state. See the Federal Bureau of Investigation CODIS Brochure, available at: http://www fbi.gov/hq/lab/pdf/codisbrochure.pdf (accessed on 21/04/2010).

86 See generally, RC Miller 'Validity, construction, and operation of state DNA database statutes' 76 ALR 5th 239 (originally published in 2000).

87 42 USC par 14132(a) (2006).

88 This would allow inclusion of DNA samples collected in terms of state and local laws over which the federal government has little or no control, including samples collected from arrestees – see Biancamano n 19 above at 620.

arrested or from non-United States persons who are detained under the authority of the United States.[89] A DNA profile can be removed from CODIS through a final court order that shows that a conviction has been overturned or that no conviction resulted from an arrest.[90]

Every state in the USA has some kind of statute that requires convicted criminals to provide DNA samples, and not only do some states already require arrestees to provide DNA samples, but there is a definite indication that more states will follow suit.[91] In California, for example, DNA samples can be obtained from all persons arrested for any felony offence,[92] while Virginia permits DNA samples to be taken from arrestees for certain violent felonies.[93] In Texas individuals indicted of certain offences, and all persons arrested for repeating crimes they have previously been convicted of, must submit to DNA testing.[94]

The constitutional validity of legislation that provides for the obtaining of DNA information in the main, has been questioned in the USA as being a violation of the right to privacy in terms of the Fourth Amendment of the US Constitution.[95] The Fourth Amendment generally protects an individual against government intrusion into his or her constitutionally protected privacy interests, and more specifically against unreasonable searches and seizures.[96] When a violation of the Fourth Amendment is alleged, it must first be determined whether a search or seizure took place. Two questions are relevant in this regard: first, does the person have a subjective expectation of privacy, and second, is that expectation of

---

89 Pub L 109–162 par 1004, codified as 42 USC par 141 35a(a)1(A) (2006).

90 See the DNA Fingerprinting Act of 2005, 42 USC pars 14132 (d)(1)–(2) (2006).

91 See generally Biancamano n 19 above at 621.

92 Cal Penal Code par 296(a)(2)(C). Louisiana has a similar law – see La Rev Stat Ann par 15: 609 (A)(1) (2005).

93 Va Code Ann par 19.2–310.2:1 (2004). Other states also require the taking of DNA samples from some classes of arrested persons – see, for example, New Mexico (NM Stat Ann par 29–16.8.1(a)(5) (2007)); Kansas (Kan Stat Ann par 21–2511(e)(1)–(2) (2007)); Alaska (Alaska Stat par 44.41.035(b)(6) (2007)); Arizona (Ariz Rev. Stat Ann par 13–610(K) (2007)); Tennessee (Tenn Code. Ann par 40–35–321(e)(1) (2007)).

94 See Tex Gov't Code Ann par 411.1471 (a)(1)(A)–(I) (2005).

95 See generally Monteleoni n 20 above at 260 etc; CJ Nerko 'Assessing Fourth Amendment challenges to DNA extraction statutes after *Samson v California*' (2008–2009) 77 *FordhamLRev* 917.

96 The Fourth Amendment states: 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

privacy one that society would consider reasonable?[97] There can be no doubt that the collection of DNA samples involves a search under the Fourth Amendment.[98]

After establishing that a search and seizure has taken place, the reasonableness of the search or seizure must be considered.[99] This consideration has been described as the 'central requirement' of the Fourth Amendment.[100] The reasonableness inquiry must examine the totality of the circumstances,[101] evaluate the degree of intrusion into the individual's privacy, and determine the extent to which the search promotes legitimate government interests.[102] If a search or seizure is found to be unreasonable, a violation of the Fourth Amendment has occurred, unless the search was conducted in terms of a search warrant supported by probable cause, or the search or seizure is justified in terms of doctrinal exceptions.[103] Such exceptions include searches conducted with consent;[104] and searches incidental to a lawful arrest[105] or special needs.[106] The special needs exception is relevant in cases where obtaining a warrant is not practical but a search is necessary,[107] or where, due to special needs, a search is necessary without reasonable suspicion.[108] It is important for the special needs to be 'beyond the normal need for law enforcement, ma[king] the warrant and probable-cause requirement impracticable'.[109] It has further been stated that the special-needs exception should be limited

---

97 See *Katz v US* 389 US 347 (1967) at 361. See generally Biancamano n 19 above at 624; Matejik n 19 above at 65; Joh n1 above at 863 etc; MA Rothstein & S Carnahan 'Legal and policy issues in expanding the scope of law enforcement DNA data banks' (2002) 67 *BrookLRev* 127 at 133 *etc*; JA Alfano 'Look what *Katz* leaves out: why DNA collection challenges the scope of the Fourth Amendment' (2005) 33 *HofstraLRev* 1017.

98 See Biancamano n 19 above at 625 and the cases to which he refers.

99 The Supreme Court has stated that a search and seizure will generally be unreasonable 'in the absence of individualized suspicion of wrongdoing' – see *City of Indianapolis v Edmond* 531 US 32 (2000) at 37. Also see *Brown v Texas* 443 US 47 (1979).

100 See *Illinois v McArthur* 531 US 326 (2001) at 330.

101 See generally *Samson v California* 126 S Ct 2193 (2006).

102 See Biancamano n 19 above at 626 etc for a discussion in this regard.

103 See *Ferguson v City of Charleston* 532 US 67 (2001) at 79–80.

104 See *Florida v Jimeno* 500 US 248 (1991) at 251.

105 See *US v Robinson* 414 US 218 (1973) at 234.

106 See *Vernonia School District 47J v Acton* 515 US 646 (1995) at 653–57; *Griffin v Wisconsin* 483 US 868 (1987) at 875 and *New Jersey v TLO* 469 US 325 (1985) at 342–43. Also see generally – J Rikelman 'Justifying forcible DNA testing schemes under the special needs exception to the Fourth Amendment: a dangerous precedent' (2007) 59 *BaylorLRev* 41 and DH Kaye 'Who needs special needs? On the constitutionality of collecting DNA and other biometric data from arrestees' (2006) 34 *JLMed&Ethics* 188.

107 See *Schmerber v California* 384 US 757 (1966) at 770–71.

108 See *Vernonia School District 47J v Acton* n 106 above at 663–65.

109 *Griffin v Wisconsin* n 106 above at 873.

to situations where the intrusion into personal privacy serves non-law-enforcement purposes.[110]

DNA sampling statutes which have been attacked have been upheld either in terms of the special-needs exception[111] or in terms of the reasonableness inquiry.[112] These cases, however, mostly dealt with the collection of DNA samples from convicted persons and the Fourth Amendment law regarding the collection of DNA samples from persons arrested[113] for, or merely suspected of, a crime remains unsettled. The courts have also failed to define a consistent standard in order to determine whether a reasonable expectation of privacy exists in such instances.[114]

Conclusion and recommendations

The proposed South African legislation will allow certain DNA samples and the information derived from such samples to be checked against the NDDSA, but only for purposes related to the detection of crime, the investigation of an offence, or the conduct of the prosecution. It is submitted, however, that the terms in which these purposes are stated are too general and might give rise to an extensive interpretation that will open up opportunities for abuse and arbitrariness.[115] Although the stated aims pursue the legitimate aims of detection and crime prevention, especially the identification of future offenders, it is submitted that these aims do not provide sufficient justification for the interference with so important a right as the right to privacy, particularly as far as mere suspects and arrestees are concerned. DNA data should be preserved in a

---

110 See *Ferguson v City of Charleston* n 103 above at 84.

111 Biancamano n 19 above at 628 points out that the 'special needs' exception is arguably unavailable to justify DNA collection statutes in light of the statements made by the US Supreme Court in the cases of *City of Indianapolis v Edmond* n 99 above and *Ferguson v City of Charleston* n 103 above, but that the open-ended nature of the doctrine does not make this conclusively the case.

112 See Biancamano n 19 above at 628 etc where he discusses the cases of *US v Kincade* 379 F 3d 813 (9th Cir 2004) (en banc); *Nicholas v Goord* 430 F.3d 652 (2d Cir 2005); *US v Stewart* 468 F Supp 2d 261 (D Mass 2007), *rev'd*, 532 F 3d 32 (1st Cir 2008). Also see K Zunno '*United States v Kincade* and the constitutionality of the Federal DNA Act: why we'll need a new pair of genes to wear down the slippery slope' (2005) 79 *St.John'sLRev* 769 at 773 etc; A Rice 'Brave new circuit: creeping towards DNA database dystopia in *US v Weikert'* (2009) 14 *RogerWilliamsULRev* 691 (discussing the case of *US v Weikert* 504 F 3d 1 (1st Cir. 2007); B Ghanaat 'Technology and privacy: the need for an appropriate mode of analysis in the debate over the Federal DNA Act' (2009) 42 *UCDavisLRev* 1315.

113 See generally *In re Welfare of CTL, Juvenile* 722 NW 2d 484 (Minn C App 2006); *Anderson v Commonwealth* 650 SE 2d 702 (Va 2007).

114 See generally Biancamano n 19 above at 628.

115 See the remarks made in *S and Marper v The United Kingdom* n 18 above at par 99.

form which permits identification of the data subjects for no longer than is required for the purpose for which the data are stored. The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage.

The evidence used in support of the retention scheme in England and Wales, which forms the backbone of the proposed scheme in South Africa, is confusing and limited, and does not convince that the scheme has significantly improved crime detection rates, beyond the rates achieved when only those profiles taken from individuals convicted of an offence of a certain gravity are retained or by simply searching against stored records, but not retaining the DNA profiles indefinitely. The blanket and indiscriminate power of DNA retention provided for by the proposed legislation cannot be justified. The mere retention and storing of personal data by public authorities, however obtained, has a direct impact on the private-life interests of the individual concerned.[116]

While nobody can deny that DNA profiles play an important part in the detection and prevention of crime, a constitutionally sound DNA collection and retention system cannot allow for the indiscriminate collection of DNA samples from all suspects arrested upon any charge. There is also no acceptable justification for the indefinite retention of such samples. It is necessary to determine the constitutional limitations of the NDDSA as far as suspects and arrested persons are concerned. Such persons may ultimately be found guilty, but they may also be found not guilty or the charges against them may be dropped. In such an instance nothing has justified their expectation of privacy being compromised.[117] This is confirmed by the fact that most DNA statutes require that DNA records be destroyed if no conviction results from a prosecution. A situation is therefore created whereby legislation that requires suspects and arrestees to submit to DNA sampling ends up targeting individuals who are not guilty of the crime of which they have been suspected or for

[116] Rothstein & Carnahan n 97 above at 167 succinctly state the crux of the matter here: 'The essence of the Fourth Amendment (and the more general principle of personal privacy) is to establish a sphere of inviolability surrounding the individual. The real question, then, is whether the government interest is so compelling as to overcome the presumption that the autonomy, dignity, and physical integrity of the individual should not be disturbed.'

[117] Compare the decision by the Minnesota Court of Appeals in *In re Welfare of CTL, Juvenile* n 113 above.

which they were arrested. Biancamano[118] points out that the defining feature of such individuals is not only that they are innocent until proven guilty,[119] but that they are not going to be found guilty of the crime for which they were arrested. Without individualised suspicion there are no compelling reasons why the state should be allowed to take DNA samples from suspects or arrested persons. If individualised suspicion is clearly present in a particular case, there is no reason why a warrant cannot be used to obtain a DNA sample.[120]

It is submitted that the Canadian approach to the collection and retention of DNA samples and profiles generally provides the best balance between the competing interests. Not only does a court have to order the collection of DNA data (thereby providing an important safeguard[121] against abuse and arbitrariness),[122] but the Canadian system also differentiates between types of offences and limits the collection of DNA data from persons who have drawn individualised suspicion. It further provides for much needed discretion when the collection of DNA evidence is at issue and further enables the police to apply for a warrant to obtain DNA samples where

---

118 Note 19 above at 644.

119 About the effect of DNA databanks on the presumption of innocence, see T Simoncelli 'Dangerous excursions: the case against expanding forensic DNA databases to innocent persons' (2006) 34 *JLMed&Ethics* 390.

120 Compare s 487.05(1) of the Canadian Criminal Code of 1985 discussed in n 70 above . Also see Matejik n 19 above at 87, who suggests that the best practice for investigators would be to obtain a search warrant from a neutral magistrate, supported by probable cause prior to obtaining a DNA sample from a suspected individual. Also see Biancamano n 19 above at 649, noting in this regard that: 'If probable cause exists, the police may absolutely get a warrant to obtain a DNA sample, but if not, the police should not be able to get that DNA through a law targeting people that are not guilty of the crime for which they've been arrested.'

121 About possible safeguards to ensure the confidentiality of DNA data – see *R v Rodgers* n 71 above at par 11; MD Herkenham 'Retention of offender DNA samples necessary to ensure and monitor quality of forensic DNA efforts: appropriate safeguards exist to protect the DNA samples from misuse' (2006) 34 *JLMed&Ethics* 375.

122 Compare the Criminal Law (Forensic Procedures) Amendment Bill of 2008, inserting section 37(4) into the Criminal Procedure Act 51 of 1977 which states that any court which has convicted any person of any offence or which has concluded a preparatory examination against any person on any charge, or any magistrate, may order that a non-intimate or an intimate sample of the person concerned be taken. Subsection 37(6)(a) further determines that intimate or non-intimate samples or the information derived from such samples, taken in terms of s 37, must be retained after it has fulfilled the purpose for which it was taken or analysed, but shall only be used for purposes related to the detection of crime, the investigation of an offence or the conduct of a prosecution. Section 37(8), however, states that despite subsection (6)(a), intimate samples and non-intimate samples or the information derived from such samples shall be destroyed after five years, if the person is not convicted by a court of law.

necessary, thereby placing a proper balance between the interests of the state and the private-life interests of suspects.

It is therefore recommended that DNA samples be taken from suspects and arrested persons in terms of a warrant.[123] Samples obtained in execution of a warrant and the results of forensic DNA analysis must be destroyed without delay when certain conditions have been met.[124] However, where an arrestee is suspected of certain sexual, violent or other serious offences that pose a threat to public safety, an extended retention period would be justified.[125]

DNA data relating to acquitted persons should be removed without delay, but there should be a time limit placed on the retention of DNA data from persons discharged either absolutely or conditionally.[126] DNA retained from convicted children[127] must be permanently removed when the record relating to the same offence is eligible to be destroyed.[128] DNA data obtained from convicted offenders should be retained indefinitely, but provision should be made for an independent body that could consider requests from individuals to have their DNA data removed from the NDDSA if special circumstances justify such removal.

---

123 Compare s 487.05(1) of the Canadian Criminal Code of 1985.

124 Compare s 487.09(1) and (2) of the Canadian Criminal Code of 1985 and s 8.1 of the DNA Identification Act of 1998.

125 Compare the position in Scotland above (at n 26 and n 57) and see s 487.09(2) of the Canadian Criminal Code of 1985 that provides for an exception in this regard – mentioned in (n 68) above. See also M Hibbert 'DNA databanks: law enforcement's greatest surveillance tool?' (1999) 34 *WakeForestLRev* 767 at 769, observing that DNA databases were originally created to help solve crimes involving certain classes of offences with statistically high recidivism rates, such as sex crimes and serious violent crimes.

126 Compare ss 9(1)–9(2) of the Canadian DNA Identification Act of 1998.

127 See the definition of a 'child' in the Child Justice Act 75 of 2008.

128 Compare s 271B of the Criminal Procedure Act 51 of 1977.