

APPLICATION NOS. 30562/04 30566/04

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

'S'

MARPER

Applicants

-v-

THE UNITED KINGDOM

Respondent

Briefing from Privacy International

For the attention of the Registrar – Mr. Johan Callewaert
Grand Chamber, European Court of Human Rights, Council of Europe
67075 Strasbourg-Cedex, France
ECHR-LE14.8bP3
KMR/MLO/s1

Contents

Data Protection and Human Rights	2
Does data about a DNA profile constitute personal data?	3
Data protection and Data retention	4
Purpose Limitations and Retention restrictions	5
Supervision of the DNA database.....	6
Unfair processing and Discrimination.....	6
Conclusions of Data Protection Analysis	8
On Leadership and International Comparisons	9
Collection.....	9
Retention of profiles from convicted offenders	9
Sample retention	9
Notes on the U.S. Perspective	10
Collection and Retention of DNA interferes with the private lives of individuals	10
Deletion provisions in U.S. federal and state laws	11
Concluding Remarks	12

1. We thank the Registrar to the Court for approving our leave to intervene in support of the Applicants in the case of *S. and Michael Marper v United Kingdom*, pursuant to Rule 44 § 2 of the Rules of Court.
2. This case is one of the most important privacy developments in recent years. The outcome of this case will determine the course of policy not just in the UK, but also across Europe and around the world. With all the privacy challenges in the past decade we have also seen strong political debate in some circumstances. However legal defenses have been weakened by inadequate policy deliberation. This is particular true in the area of informational privacy.
3. Informational privacy and its regulatory regime, data protection law, needs stronger support to deal with contemporary challenges. The collection, processing, and retention of genetic data is threatening the same legal regime that protects abuses of communications data, financial data, and sensitive data including medical, political and religious data. There are initiatives across the world to also bring these varying types of data together and conduct in-depth analyses.
4. In our intervention we show the firm relationship between data protection law with Article 8 of the European Convention on Human Rights. We do so to argue that the UK Government fails to adequately address the key ECHR tests. We also show that the UK regime of protections is immature and in need of significant changes to even catch up to the most primitive safeguard regimes elsewhere.

Data Protection and Human Rights

5. In this section we argue that Data Protection and Human Rights legal instruments interact with one another in order to ensure for the protection of privacy. In their decision regarding this case, the UK House of Lords did not consider any of the UK Government's data protection obligations. We contend that the European Court can consider data protection, under both the Council of Europe Convention 108 and the UK Data Protection Act. Given the overlap between human rights and data protection, the case before the Court provides an opportunity for clarifying how these laws regarding the collection, processing and retention of DNA have an impact on private and family life.
6. Data protection laws across Europe follow from the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.¹ This was then followed up by the European Union with its Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which in its preamble notes that the Directive enunciates a number of privacy principles in order to “give substance to and amplify those contained in the Council of Europe Convention”.² The EU Directive also claims that the object of national laws on data protection is to protect fundamental rights and freedoms, and in particular Article 8 of the ECHR. The EU Directive is the direct basis for national law across the EU, seeking “to ensure a high level of protection in the Community”, culminating in the UK Data Protection Act 1998.
7. Human Rights and Data Protection are often cited together as complementary or supplementary. This is repeatedly done in Council of Europe conventions and recommendations that relate to the processing of personal information, for instance on genetic testing,³ biomedicine,⁴ and DNA analysis within the criminal justice system.⁵ In arguing that the ECHR “is supplemented, extended and reinforced by other conventions, with other methods of supervision”, Justice

1 Strasbourg, 28.I.1981, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

2 Preamble 11, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

3 Council of Europe, Committee of Ministers, Recommendation No. R (92) 3 on Genetic Testing and Screening for Health Care Purposes, February 10, 1992.

4 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997.

5 Council of Europe recommendation No.R(92)1 of the Committee of Ministers to Member States on the Use of Analysis of DNA Within the Framework of the Criminal Justice System, February 10, 1992.

Francoise Tulkens contends that the data protection Convention 108 “secures, in that domain, protection of private life.”⁶

8. Though the two instruments often apply in the same circumstances, we wish to point out the essence of the relationship. The functional difference between the ECHR and Data Protection law is determined by considering the main purpose of the respective legal obligations. The main focus of the Article 8 obligations is to assess whether any interference by a public authority is lawful by reference to the tests posited by Article 8(2). The tests posited by Article 8(2) focus on whether personal data are lawfully processed.⁷ Data protection, on the other hand, looks at how we may assess those tests.

9. Any interference with the Article 8 right must pass three legal tests. Is the processing of personal data in accordance with law? Is the law pursuant to one or more of the interests of the legitimate objectives identified in Article 8(2)? Is the law necessary in a democratic society in those cases where personal data are processed? In this way, it can be seen that the data protection obligations sit underneath Article 8, and are essential for determining the proportionality of the processing. This assessment takes place by reference to a number of data protection principles which relate to not whether personal data should be processed but rather how personal data are processed. The principles establish fair processing requirements in relation to issues such as openness and transparency; fairness and lawfulness of the activities; rights of access to personal data; collection limitations (only that data which is necessary is collected); purpose limitations (data collected for a purpose is used only for that purpose); security and accuracy assurances; limited use, disclosure, and retention; and enforceability and verifiability of compliance with these requirements. Proportionality is thus assessed by considering each of these data protection principles.

10. It can thus be argued that if there are significant departures from the data protection law and principles, then this is a strong signal that the processing could well be disproportionate in terms of Article 8. If there are very few departures, by contrast, then this is a strong signal that the processing is proportionate.

11. Below conduct this proportionality analysis by apply the key questions emerging from data protection law to the situation under consideration in this case, and show that the UK practices are disproportionate.

Does data about a DNA profile constitute personal data?

12. One of the key challenges is establishing whether DNA qualifies as personal data under data protection law. The definition of personal data under the UK Data Protection Act 1998 is:

“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.

13. The Council of Europe Convention No. 108 states that for the purposes of the convention:

"personal data" means any information relating to an identified or identifiable individual ("data subject").

14. A DNA sample is widely believed to be unique for an individual, save for identical twins. Therefore the digital representation of that DNA pattern derived from a sample of DNA (e.g. found at the scene of crime) is also unique and is *intended* to relate to a specific individual.

6 Francoise Tulkens, ‘Human rights, rhetoric or reality?’, *European Review*, Vol. 9, No. 2, 125–134, 2001.

7 “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,

15. In the case of the DNA found at the scene of a crime which relates to an unknown individual, the police are very likely to want to establish the identity of the individual concerned, so that he or she – assuming that person to be a suspect - can be arrested, by the police, at a later stage of the investigation. The intention is to identify the individual concerned. Meanwhile, volunteer data is taken for a number of reasons including “to identify persons involved in criminal paternity cases, familial searches and for identification of victims of mass disasters.”⁸

16. The fact that the UK DNA database is linked to the UK Police National Computer provides evidence of linking the DNA digital representation to other name-linked personal data. The UK police’s “DNA Good Practice Manual”⁹ states that DNA should not be taken from an “Arrestee or Volunteer” if there is a marker on the PNC stating that a DNA profile is already held.¹⁰

17. It follows that the digital representation of a DNA sample is personal data in terms of the Council of Europe’s definition. Additionally in the case under consideration by this Court, the police will have other information in its possession which relates the digital representation in the DNA database to other information about Mr. Marper. It follows that such data are also personal data and the data protection requirements of the Convention are engaged. And if data protection legislation is engaged, it also follows that Article 8 of the ECHR is engaged.

Data protection and Data retention

18. The general data protection obligation relating to the deletion or retention of personal data by a data controller (the organisation responsible for the processing of personal data) requires personal data to be deleted when its retention can no longer be justified by a data controller. Article 5 of the Council of Europe Convention No 108 expresses this proposition by stating that personal data shall be “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”. The UK Data Protection Act 1998 implements this requirement in the Fifth Data Protection Principle which states: “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.

19. The UK Government’s position appears to be that the retention of DNA personal data is always relevant to the policing purpose so it follows that the DNA personal data need not be deleted. By contrast the Council of Europe recommendation R(92)1 on DNA use in the criminal justice system takes a different view.

20. R(92)1 recommends in paragraph 8, that “measures should be taken to ensure that the results of DNA analysis are deleted when it is no longer necessary to keep it for which it was used”. This, to make sense, infers a retention period which is shorter than the life time of the data subject because otherwise this recommendation would be otiose. Paragraph 8 also recommends “strict storage periods”. In general, paragraph 8 infers that DNA personal data are deleted after some time-limit. The usual practice in the UK, by contrast, is to retain DNA personal data indefinitely, including after the death of data subject, for a period which is not determined by a law. The police do permit samples to be deleted from the DNA database, but only if exceptional circumstances apply.¹¹

21. R(92)1 also recommends, in paragraph 8, retention of DNA in cases of serious offences (“where the individual concerned has been convicted of a serious offence”) or where the security of the state is involved. Yet the UK practice is to retain indefinitely DNA personal data in all circumstances (including after the death of data subject). The Recommendation also carries the implication that in cases where less serious offences have been proved to have been

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”.

⁸ DNA Good Practice Manual, Second Edition 2005, published by the Association of Chief Police Officers (ACPO), available at http://www.acpo.police.uk/asp/policies/Data/dna_good_practice_manual_2005.doc

⁹ *ibid*.

¹⁰ Paragraph 4.5 – DC means DNA confirmed, DP means sample on the database, DT means sample taken but not profiled etc

committed, DNA profiles and related DNA personal data should not be retained beyond a reasonable time which has been established by law. If this is the case, it follows that DNA data from those acquitted or not proceeded with should also be deleted after a reasonable time.

22. R(92)1 recommends in paragraph 8, that DNA personal data can be retained if the individual concerned "so requests". Any normal interpretation of this provision would include the prospect that individuals who provide samples can change their mind, and if they do so, the personal data related to the sample and the sample itself are deleted. If R(92)1 wanted to adopt the UK position, it would have included the word "indefinitely" in its text. A UK Parliamentary Committee has commented that it cannot understand the Government's position on consent.¹² It has stated that "We do not understand why consent should be irrevocable for individuals who are giving DNA samples on a voluntary basis". By contrast, the Government claims that (a) it would hinder the administration of justice if samples which should have been destroyed were in fact retained and then subsequently challenged; that (b) the withdrawal of consent is a precursor to criminal activity and that (c) it is administratively convenient¹³ to keep the DNA data, as the law abiding person has nothing to fear. Paragraph 8 of R(92)1 does not make reference to the above criteria as justifying retention of DNA personal data; by contrast it sets out "strict limits" on the retention of such data.

23. R(92)1 recommends in paragraph 8, that "where the security of the state is involved, the domestic law of the member state may permit retention of samples ... even though the individual concerned has not been charged or convicted of an offence". The Recommendation continues: "In such cases, strict storage periods should be defined by domestic law." The practice in the UK differs from the Recommendation as the purpose of the indefinite retention is not limited to state security, storage periods have not been defined in domestic law, and DNA personal data are retained even after the death of the individual.

24. This interpretation of the problems with retention with respect to data protection is widely understood. For instance, in Greece in 2001 the Greek Data Protection Authority ruled specifically on these grounds, by ruling that DNA should be destroyed once the fulfillment of the intended aim is achieved.¹⁴ Additionally, the DPA ruled against any effort to collect and analyse genetic material for preventative purposes.¹⁵

Purpose Limitations and Retention restrictions

25. According to section 3 of R(92)1 DNA personal data should not be used for other (non-policing) purposes. Samples collected for one purpose may only be used for another purpose "in circumstances laid down expressly by the domestic law". Restrictions on the retention of DNA personal data are essential safeguards for this obligation to limit purpose-creep: if DNA personal data are retained, then the potential for wider use of DNA personal data is omnipresent. If personal data are deleted, they cannot possibly be used for other purposes.

26. Note that the Recommendation also excludes other purposes which could be permitted under Article 8(2) – for example, the use of DNA samples compiled by the police for a future public health purposes. The Recommendation is therefore very restrictive on the use of DNA from any further use for a different purpose. This is another example as to why DNA is obviously in a unique position because the potential for wider use of DNA personal data is both obvious and transparent.

11 Williams R (2007) 'Orwellian' CCTV in shires alarms police officer. The Guardian, 21 May 2007. <http://www.guardian.co.uk/humanrights/story/0,,2084290,00.html>

12 Paragraph 75 of House of Commons Science and technology committee's Seventh Report of Session 2004-05 entitled 'Forensic Science on Trial', March 16 2005.

13 Government Reply to the Select Committee Report in reference 13

14 Hellenic Data Protection Authority. Opinion.15/2001, available at <http://www.dpa.gr/decision_eng.htm>.

15 Id.

27. In the UK House of Lords judgement¹⁶ however, that Court determined that because the law prohibited wider use of the sample or data, and because the data did not reveal medical implications¹⁷, and because the Court could revisit its decision if there were to be further use¹⁸, then it followed that the Court could ignore this concern. This does not reflect our analysis of R(92)1 nor Convention 108.

Supervision of the DNA database

28. R(92)1 recommends in paragraph 4, that DNA analysis should only be carried out in circumstances determined by domestic law. UK law does not differentiate between fingerprints and DNA samples. Treating them the same under law ignores the significant differences between them.

29. For instance, the police have now started to make use of familial testing of DNA (when the DNA of one individual is related to another), and additional research purposes. The UK Parliament Science and Technology Parliamentary Select Committee¹⁹ commented on this point, stating:

“It is extremely regrettable that for most of the time that the NDNAD has been in existence there has been no formal ethical review of applications to use the database and the associated samples for research purposes. The recent initiation of negotiations with the Central Office for Research Ethics Committees is too little too late.” (Paragraph 82)

“We are concerned that the introduction of familial searching has occurred in the absence of any Parliamentary debate about the merits of the approach and its ethical implications.” (Paragraph 84)

“Any future extension to the applications for which the data in the NDNAD can be used must be subject to public scrutiny.” (Paragraph 85)

“In failing to respond more positively to the calls for independent oversight of the database, the Home Office gave the impression that it was not a high priority.” (Paragraph 77)

30. It is noteworthy that Paragraph 50 of an Explanatory Memorandum to R(92)1 states that, if exceptions to the deletion rule are being considered, then the storage of DNA personal data should be subject to control by Parliament. If there were effective oversight arrangements and Parliamentary control, then it is our belief that the UK Parliamentary Committee would not have made such comments.

Unfair processing and Discrimination

31. The first principle in Article 5 of Convention No 108, (implemented in the Data Protection Act 1998 by the First Principle) requires "Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully". This in turn requires consideration of the concept of "fair processing".

32. In the UK, in case of MDU v Johnson²⁰, the concept of fair processing arose in a case where it was argued that the outcome of the processing of personal data caused an individual particular detriment. The case involved the use of a risk assessment system by an insurer, the use of which resulted in a health professional having his medical insurance cover withdrawn. The health professional sued for damages and argued that the outcome of the processing was unfair because he had been subject to a faulty risk assessment procedure. The Court's judgment was that the processing was fair because the risk assessment procedure had been applied to everyone who had applied for insurance.

33. The Court commented in this case:

"123. It is easy to see how he regards the decision in his case as unfair but it has to be remembered that the policy is directed at risk management – at preserving the MDU funds against a risk of claims, and the

16 Para 28, Marper case, [2004] UKHL 39

17 Para 29, Marper case, [2004] UKHL 39

18 Para 86 (for example), Marper case, [2004] UKHL 39

19 "Forensic Science on Trial", session 2004-2005, March 16 2005.

20 David Paul Johnson V The Medical Defence Union Limited, Neutral Citation Number: [2006] EWHC 321 (Ch)

incurring of costs, in the future.....The MDU is entitled first to determine its policy. Having done so, it then has to ensure that any processing of members' data in line with that policy is carried out fairly".

34. It is this concept of "fairness" (whether a process applies to all data subjects or a subset of a population of data subjects) which comes into contention when considering the DNA database.

35. There is mounting evidence that the UK DNA database has registered a disproportionate number of black men. Within the Metropolitan Police area, 51% of the innocent (uncharged) people whose DNA is held on the Database are of black or BME origin.²¹ This disproportionate representation of black men on the Database exacerbates and reinforces discriminatory police practices which are well-documented.

36. Action on Rights for Children (ARCH), in its submission to the Nuffield Council²² stated that "Arrests and disposals: 10-17-year-olds 2005" that the provisional figures indicate that 348,000 (or 24%) of all arrests in 2005 were of 10-17s.²³ They state that 118,900 10-17s received reprimands (69%) or final warnings (31%)²⁴ and 96,300 were convicted in the courts²⁵. This means that "Thus in total there were 215,200 disposals, and 132,800 arrests did not lead to any disposal". ARCH adds: "The 2004 figures are remarkably similar to the 2005 figures above, when 330,800 arrests led to 195,500 disposals. 135,300 arrests did not lead to disposal".

37. The rising arrest rate occurs against a background of criticism of the Government 'Offences Brought to Justice' (OBTJ) targets. The Police Federation of England and Wales asserts that these targets incentivise arrest for low-level offending²⁶; the former Chair of the Youth Justice Board, Professor Rod Morgan, has said: "Many, though not all, police forces are picking a lot of low-hanging fruit — the lowest of which comprises juvenile group behaviour in schools, residential homes and public spaces — to meet their OBTJ targets."²⁷

38. During 2006/07, repeated requests were made to the Home Office by Parliamentarians and by ARCH for the number of children who had not received any disposal by way of criminal conviction, reprimand or final warning, but whose DNA profiles were retained on the national DNA database. Following the intervention of the UK Children's Commissioner, the Parliamentary Secretary of State at the Home Office indicated that 358,012 DNA profiles related to 10-17-year-olds. Of these, 81,750 did not have any conviction, reprimand or final warning. The Home Office applied a replication rate of 13.7% to reduce this figure to 32,953.

39. In this same letter, the Secretary of State asserts that it is: "ultimately an operational decision for the police whether to take a sample". ARCH has since then contacted all police forces in England and Wales; none has any specific policy relating to the collection and retention of DNA samples of children and young people under 18.

40. Figures up to 2007 show that 1,125,141 of those on NDNAD were added when under 18; and 521,901 added when under 16.²⁸

41. With familial techniques developing, the taking of DNA of a young person will map that person's family as well. This in turn leads to the question of whether the processing of personal data in these circumstances is fair.

42. For example, if the DNA database spanned a significant proportion of a particular minority grouping based on race, there is a risk that the police could target members of that community on the grounds that gradually, with familial testing taken into account, the possession of DNA personal data will span the whole of that community and ease

21 Liberty's response to the Home Office Consultation: "Standard Setting and Quality Regulation in Forensic Science", November 2006, available at <http://www.liberty-human-rights.org.uk/pdfs/policy06/forensic-science-regulator.pdf>

22 In its study of "The Forensic Use of Bioinformation: Ethical Issues".

23 Home Office Statistical Bulletin: Criminal Statistics 2005, England and Wales 19/06

24 Ibid (Table 3A, paras 3.18 and 3.19)

25 Ibid (Table 3.7)

26 'Police condemn target culture', <http://news.bbc.co.uk/1/hi/uk/6656411.stm>

27 Royal Society of Arts Journal, July 2007

28 Response by John Reid, Home Secretary, to Parliamentary Question from David Davis, May 10 2007, pt 0019, available at <http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070510/text/70510w0019.htm#070510114000148>.

detection of crime within that community. The point being raised here is that the case can be argued, following *MDU v Johnson*, that if DNA is retained disproportionately amongst certain members of the society, with the result that this community is targeted by the police, then this would qualify as unfair processing under data protection law.

43. Finally, there is an argument which says that the risk of unfairness can be alleviated if DNA from the whole population is taken, irrespective if there is a crime committed or not. As everyone is on the database, so the argument goes, the procedures have been applied to all and that there would be no stigma attached in relation to a DNA profile being held by the police. However, such a policy could give rise to a new face to unfairness – in that it presents the criminal with the ability to leave someone's DNA at the scene of a crime, with the certainty that these individuals will be investigated.

Conclusions of Data Protection Analysis

44. Data protection law would not preclude the taking of a DNA sample from somebody arrested and using information derived from that sample in relation to an inquiry. Nor would data protection law prevent DNA personal data derived from a sample being processed and comparisons been made with samples found at the scene of a crime or other scenes of crime. Data protection law would not require DNA personal data to be deleted by the police, if such data could be justified in terms of their current inquiries.

45. In general, where the retention of DNA personal data could not be justified in terms of current inquiries, a data protection analysis would derive a range of different retention periods for the personal data. The retention time would depend on a number of factors such as the status of the data subject (convicted, arrested), the likelihood of recidivism, the age of the data subject, the length of time which had passed since the data subject last came to police attention, and the seriousness of the crime involved or being investigated.

46. Such factors are apparent from published criminal statistics. For example, criminal statistics relating to those born between 1953 and 1978 reveal that "the majority of offenders had been convicted on only one occasion" and that "the peak age of known criminal activity for males was nineteen".²⁹ If this is the case, data protection would require consideration of the deletion of DNA personal data if (a) the offence was minor; (b) the offender had not repeated a crime; (c) the offender was of a certain maturity (e.g. over 30), and that the police had not interest in the data subject.

47. So for example different retention periods relating to the DNA personal data and samples would likely to differentiate between groupings such as:

- those identified individuals who are convicted of minor offences.
- those identified individuals who are convicted of serious offences.
- juveniles who are processed by the criminal justice system .
- those identified individuals who are arrested and whose DNA matches that found at another scene of crime.
- those identified individuals who are arrested but are not convicted or proceeded against.
- those identified individuals whose samples need to be eliminated from the DNA found at the scene of crime.
- those unidentified individuals whose DNA is found at the scene of a crime.
- those who consent to the DNA personal data being processed.

48. Sometimes there may be overlap. For example, DNA personal data in category (b) and (g) are likely to be kept indefinitely whereas (h) would be retained until consent is withdrawn; some special rules might apply for category (c) and the retention times for (a) would be longer than (e). However, this approach appears not to be consistent with the

²⁹ <http://www.homeoffice.gov.uk/rds/pdfs/hosb401.pdf>

current UK approach of "one size fits all" and where all DNA personal data in the above categories are kept indefinitely.

On Leadership and International Comparisons

49. The UK Government asserts that it is merely leading the world as a pioneer in the field of DNA collection, processing, and retention. In fact, the UK DNA Database's legal standing is arguably primitive when compared to the legal bases in other countries. Other submissions to this court have shown variances around the world on legal safeguards and protections, in particular the witness statement from Caoilfhionn Gallagher and the research from the Nuffield Council Report.³⁰

50. While the experiences of other countries may go some way to informing the deliberation on this case, and showing that other countries have at least considered data protection and thus proportionality, the outcome of this case will have serious implications for human rights in other countries. Countries around the world are looking to the UK for potential leadership. Recently Malaysian officials have referred to the UK model as ideal, celebrating the UK's claims of crime-matches without any level of scrutiny for detail.³¹

51. In this section we will draw out the key points to be learned from international comparisons.

Collection

52. The UK collection and retention practices goes far beyond most of those in other European countries. For instance in Austria DNA sampling is limited to persons suspected of "severe" crimes (crimes against persons). Several countries limit sampling to crimes that attract specific terms of imprisonment as punishment (Finland – 6 months; Norway – 2 years; Sweden – 2 years; Netherlands – 4 years³²; Hungary – 5 years; Belgium – 5 years). Meanwhile, Estonia, Latvia, and Lithuania collect data from anyone suspected of a crime. On the other hand, in Germany a suspect must be deemed to be at risk of committing a recordable offence in the future before their profile can be entered into the database.

Retention of profiles from convicted offenders

53. To our knowledge, Austria, Estonia and Finland also indefinitely retain profiles. Yet a number of countries have set retention limits. These include: Sweden (10 years after the end of the sentence), Israel (20 years),³³ Hungary (20 years), France (40 years), the Netherlands (depending on the severity of the crime), the Czech Republic (three year reviews after conviction), and Belgium (indefinite retention only for those convicted of some violent or sexual crimes). Some states require suspects or prosecuting authorities to request removal once proceedings are ended.

Sample retention

54. The UK appears to be alone in retaining the DNA samples. The nearest exception is that in Switzerland the destruction of the sample takes place within three months after entering the profile on the database.

55. Therefore, other than England and Wales, no jurisdiction to our knowledge systematically retains the profiles or samples of individuals who have not been convicted of a crime.

30 C.f. page 52, box 4.3 of the Nuffield Council on Bioethics, 'The forensic use of bioinformation: ethical issues', September 2007.

31 'Forensic DNA databank soon', Elizabeth John and Sonia Ramachandran, The New Straits Times, January 20, 2008.

32 "DNA Samples to be Taken from Convicted Persons," Ministry of Justice, February 2005, available at <<http://english.justitie.nl/currenttopics/pressreleases/archives2005/Dna-samples-to-be-taken-from-convicted-persons.aspx>>.

33 Jonathan Lis, "Police to start DNA Bank of Suspects, Convicts," Ha'aretz, June 15, 2005.

Notes on the U.S. Perspective

56. While the UK hopes to claim the status of pioneer and thus is most advanced, in fact the U.S. has been conducting DNA analysis just as long, and even though data protection rules do not apply in the U.S., there are much greater safeguards.

Collection and Retention of DNA interferes with the private lives of individuals

57. The highly sensitive nature of DNA personal data has been widely recognized. For the past several years, the U.S. Senate has unanimously approved legislation that seeks to protect individuals from genetic discrimination in the contexts of employment and health insurance.³⁴ There is a general agreement that the collection of DNA interferes with constitutional rights and protections. The Fourth Amendment of the U.S. Constitution guarantees “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”³⁵ The conduct of a “search” generally requires probable cause and a judicial warrant, or at least individualized suspicion.

58. In cases where forensic DNA databases have been challenged on the grounds of the Fourth Amendment, the courts have generally agreed that the taking and analysis of one’s DNA constitutes a “search” for one of two reasons. First, bodily intrusion is necessary for collecting a blood or buccal swab sample for use in DNA testing. Second, the substantial and uniquely personal information contained in the DNA itself has been found to trigger protections guaranteed under the Fourth Amendment.³⁶

59. However, U.S. courts have generally upheld the operation of DNA databases of *convicted offenders* for one of two reasons: because the government’s interest is one of “special needs, beyond the normal need for law enforcement”³⁷ or because convicted felons have a “diminished expectation” of privacy, as balanced against society’s need to promote law and order.³⁸ Arguably, the role of DNA databases for convicted felons is for precise identification and for helping police solve recidivist crimes.

60. Courts that have upheld DNA database statutes based on the “special needs” exception have had difficulty explaining why the government’s interest in identifying and prosecuting criminals and determining recidivist acts were interests beyond “normal law enforcement.”³⁹ Furthermore, two recent Supreme Court rulings have further narrowed the scope of the “special needs” exception in ways that call into question whether this exception should apply at all to DNA databanks. In *City of Indianapolis v. Edmond* and *Ferguson v. City of Charleston*, the Court found that where the primary purpose of a program involving a search is related to the general interest in crime control, the “special

34 Legislation to ban genetic discrimination was first introduced in the 104th Congress in 1996. The bill under current consideration is S. 358, the Genetic Information Nondiscrimination Act of 2007, introduced by Senator Snowe. S. 358, 110th Cong. (2007).

35 U.S. Const. amend. IV.

36 See, e.g., *Jones v. Murray*, 962 F.2d 302, 306 (4th Cir. 1992); for a detailed overview of legal challenges relevant to DNA testing and retention, see Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 *Brook. L. Rev.* 127 (2001).

37 *State v. Olivas*, 856 P.2d 1076, 1085 (Wash. 1993) (upholding the Washington DNA testing statute, stating that the purpose of the DNA data bank was to deter and prosecute recidivist acts, and that this purpose was a “special need” of government beyond normal law enforcement).

38 See, e.g., *Landry v. Att’y Gen.*, 709 N.E.2d 1085, 1092 (Mass. 1999); see also *Hudson v. Palmer*, 468 U.S. 517, 523 (1984); *People v. Wealer*, 636 N.E.2d 1129 (Ill. App. Ct.); *Jones*, supra note 6, at 308.

39 For example, in *Shelton v. Gudmanson*, the court found that Wisconsin’s DNA testing of prison inmates was related to law enforcement, but allowed it to be considered within the “special needs” exemption because it was “not undertaken for the investigation of a specific crime.” 934 F. Supp. 1048, 1050 (W.D. Wis. 1996).

needs” exception under the Fourth Amendment does not apply; in that circumstance a warrant supported by probable cause is required.⁴⁰ The issue of the legality of DNA databases has not been heard by the U.S. Supreme Court.

61. Regardless of whether a DNA database should be considered beyond the general needs of law enforcement, the proposition that the government’s “special needs” outweigh the privacy interests of innocent persons seems beyond the pale, as a matter of Constitutional principle. While it is plausible that the courts could uphold the forcible taking and analysis of DNA of persons arrested on the basis of some diminished expectation of privacy while in confinement, the permanent retention of that DNA cannot be justified on this basis unless a suspect is convicted of a crime.

62. The issue of whether DNA can be retained from persons who were arrested and/or charged but *not* convicted of a crime has almost never been tested in U.S. courts. This is because the majority of U.S. states have not expanded their DNA databases beyond convicted felons. Such proposals have been met with significant public opposition. Last year, South Carolina Governor Mark Sanford vetoed legislation to allow DNA collection from anyone arrested, stating, “A DNA sample [as compared to a fingerprint] contains a great deal of sensitive personal information... permitting law enforcement to attain DNA samples during warrantless arrests stretches the boundaries of being constitutional.” Many scholars have predicted that authorization of DNA sampling and retention of individuals who are not convicted of a crime should be held unconstitutional.⁴¹

63. In the one case where DNA retention of non-convicted individuals has been tested, it has been struck down. In 2006, Minnesota’s Court of Appeals held that taking DNA from juveniles and adults who have had a probable cause determination on a charged offence but who have not been convicted violates state and federal constitutional prohibitions against unreasonable searches and seizures.⁴² In particular, the court found that the state’s interest in collecting and storing DNA samples is outweighed by the privacy interest of a person who has not been convicted.⁴³

Deletion provisions in U.S. federal and state laws

64. U.S. federal law requires destruction of DNA identification records of individuals in the database upon receipt of a certified copy of a final court order establishing that the conviction was overturned. 42 USCA § 14132(d)(1).

65. As a condition of access to the Combined DNA Index System (CODIS), federal law also requires that states promptly expunge from the index the DNA analysis of a person included in the index if the State receives a certified copy of a final court order establishing that such a conviction was overturned or that the person was not convicted of an offence and all charges against the person were dismissed or resulted in an acquittal. 42 USCA § 14132(d)(2).

66. Most state statutes contain provisions allowing for individuals to petition to have their DNA samples and profiles and accompanying records destroyed upon reversal of a conviction or case dismissal.⁴⁴

40 Under *City of Indianapolis v. Edmond* the Court struck down a program in which police used dogs to sniff for drugs in vehicles pulled over in groups at fixed roadblocks because they found the primary purpose of the checkpoint program to be related to the general interest of crime control. 531 U.S. 32 (2000). Similarly, in *Ferguson v. City of Charleston*, the court struck down a program in which a university hospital tested urine samples from pregnant women for cocaine and reported positive results to the police because the primary purpose of the program was said to be the arrest and prosecution of drug-abusing mothers, and therefore in the general interest of crime control. 532 U.S. 67 (2001).

41 See for example, 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?” *Journal of Law, Medicine & Ethics* 33, no. 1 (2005): 102-224. Report in *Journal of Law, Medicine & Ethics* 34, no. 2 (2006): 165-187.

42 *In re Welfare of C.T.L.*, 722 N.W.2d 484 (Minn. Ct. App., 2006).

43 *In re Welfare of C.T.L.*, supra note 13.

44 For detailed information on the span of state provisions, see: http://www.aslme.org/dna_04/grid/statute_grid_4_5_2006.html

Concluding Remarks

67. According to the 2002 global survey by Interpol, 77 of its 179 member countries perform DNA analysis and 41 member countries have a functioning DNA database.⁴⁵ As of 2003, 36 of 46 European Interpol members perform forensic DNA testing, and 26 of them allow international exchange of information.⁴⁶ At the time, Interpol predicted that the percentage of members having DNA databases would double in the next few years.

68. Yet DNA is personal data, and thus processing must comply with data protection law. The practices of the UK are disproportionate, and this is in part because of ineffective Parliamentary controls. Relying merely on Parliamentary processes in this highly complex arena has to date resulted in very mixed results around the world. Somehow the UK Government must be compelled to limit retention periods and apply retention only to convicted data, limit collection, and limit processing particularly in the light of the remarkable number of children who are on the DNA database.

69. Most worryingly the UK has been arguing that it has set the standard for genetic data processing. Governments across Europe and around the world are watching the UK, and using its same obscure facts to justify unlawful data processing. To correct the direction in which we are all heading, strong leadership is required, and an open political debate unlike any other that we have seen in modern times must occur. Strong legal protections are needed to reign in these developments and set us on the right course.

45 Interpol, "Global DNA Inquiry Results 2002" <<http://www.interpol.int/Public/Forensic/dna/inquiry/default.asp>>.

46 Christopher H. Asplen, "International Perspectives on Forensic DNA Databases," ISRCL Conference, The Hague, August 24-28, 2003.