APPLICATION NOS. 30562/04 30566/04

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

(1) 'S'
(2) MARPER

Applicants

-v-

THE UNITED KINGDOM

Respondent

RESPONSE TO QUESTIONS POSED BY THE COURT UPON THE ISSUE OF ITS DECISION ON ADMISSIBILITY AND FURTHER SUBMISSIONS

Introduction

1. On 16 January 2007 the Court declared the above applications admissible, and invited the parties to submit additional observations on the questions set out in an annex to the letter informing the parties of the admissibility decision. The court also stated that it was open to the parties to submit any other evidence or additional observations relating to any aspect of the case.

2. The Court also asked for observations as to whether there should be an oral hearing in this matter, and also reminded the applicants that they should submit their claims for just satisfaction pursuant to Rule 60 of the Rules of the Court.

3. In this document the Applicants address all these points. Also submitted is a detailed statement from Dr Caoilfhionn Gallagher which

sets out detailed background to the history, statutory framework, and practice of retention of samples, profiles and fingerprints. The statement also contains a detailed analysis of the comparative context of the retention of this material both in Europe and elsewhere in the world. The statement is referred to at various points throughout these submissions. There are also three exhibits to the statement which are referred to herein. The statement and exhibits are commended to the court.

4. In relation to an **oral hearing**, the Applicants' case is that the complexity of the issues raised, the importance of the Court reaching a fully informed decision, and the wide-ranging comparative aspect of the case that the Court has invited the parties to address, all mean that an oral hearing in this matter would be appropriate.

5. It may well be that the Court will need to be updated on a number of issues prior to making a decision, and this will also make an oral hearing important. For example, the Court has expressed an interest in the comparative position. Dr Robin Williams published an interim report in June 2005 funded by the Wellcome Trust entitled *Forensic DNA Databsing: A European Perspective* http://www.dur.ac.uk/resources/sass/Williams%20and%20Johnson%20Interim%20Report%202005-1.pdf. This is the definitive European comparative work but the final report is due in May 2007.

6. The Applicants deal with the issue of **just satisfaction** towards the end of these submissions.

The Court's questions

The Court has asked the parties to address whether the retention of the applicants' (a) fingerprints, (b) DNA profiles and (c) DNA samples involves

an interference with the right to respect for their private and family life as guaranteed under Article 8 ECHR.

7. This point has been covered in the application and the applicants' response to the Government's observations at the admissibility stage. However, the Court has raised further relevant documents and cases as follows:

   (a) Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal date;
   (b) *Sciacca v Italy,* App. No. 50774/99, Judgment of 11 January 2005 (concerning fingerprints);
   (c) *Van der Velden v Netherlands*, App No 29514/05, Judgment of 7 December 2006 (concerning DNA information).

8. In summary, it is submitted that retention of fingerprints, profiles or samples when the original purpose for collection has dissipated constitutes a fresh interference with the subject's right to private and family life under Article 8(1) ECHR. (Such a fresh interference must also, of course, be subjected to fresh Article 8(2) analysis.)

9. This approach has been consistently endorsed by Council of Europe Recommendations and Conventions since 1968; it is in line with recent jurisprudence of the European Court of Human Rights; it also follows the careful, nuanced approach adopted by courts in other jurisdictions, in particular the Supreme Court of Canada and the German Constitutional Court.

10. If, as the Respondent Government now accepts, the initial enforced collection of the biometric material (fingerprints or samples) constitutes a *prima facie* interference with Art. 8(1), but that interference is justified under Art. 8(2) as necessary and proportionate in order to investigate a specific criminal offence, the retention of that

information after the basis for the Art. 8(2) justification has vanished must raise fresh Art. 8 questions. The Respondent Government's repeated references to "mere retention" of this material are misconceived, as they have failed to recognise that not only does the initial taking constitute an interference with the physical or bodily integrity of the individual, an aspect of the right to private life under Art. 8(1), it also interferes with the individual's informational privacy and his or her right to informational self-determination, further aspects of the right to private life.[1]

11. These aspects of privacy have been described by La Forest J of the Canadian Supreme Court:[2]

> "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" (*R v Dyment* (1988) 45 CCC (3d) 244, at 255-256).

12. It is submitted, as a general principle, that the retention of fingerprints, profiles and samples clearly constitutes a continuing interference with the Applicants' rights to informational privacy and informational self-determination under Art. 8(1).

13. The Applicants note that the Court has on many occasions accepted that, although the original action in obtaining information relating to an individual may either not engage Art. 8(1) or it may be justified under Art. 8(2), further processing or dissemination of that information may breach Article 8: *Peck v. UK* (2003) 36 EHRR 41; *Sciacca v. Italy*, App. No. 50774/99, Judgment of 11 January 2005. In these cases the later event was active – the dissemination of videotape footage (*Peck*) or the distribution of a photograph from a police file to journalists (*Sciacca*) – but it is submitted that continuing storage of personal information as in the present case also interferes with Art. 8(1).

[1] See further Dr. Gallagher's outline of the five aspects of privacy at paras. 269-292 of her statement.
[2] And see also the comments of Baroness Hale, para 69 of the House of Lords judgment.

14. This is in keeping with the guiding principles of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "Data Convention") (opened for signatures 28th January 1981; came into force 1st October 1985) referred to by the Court in its questions.

15. . This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data. The Preamble includes the following

> Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.

16. It establishes that personal data should be processed fairly and lawfully (Article 5(a)), must be stored for specified and legitimate purposes (Article 5(b)), must be "relevant and not excessive in relation to the purposes for which they are stored" (Article 5(c)) and, crucially, must 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" (Article 5(e)).

17. It is submitted that the Convention No. 108 principles are readily applicable to the materials and information in this case (fingerprints, profiles and samples). It applies to "the automatic processing of personal data" (Article 1) and "personal data" are defined in Article 2(a):

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

18. Article 2 is broadly drawn, applying to "*any* information" and "*identifiable*" individuals. It is submitted that fingerprints, profiles and

samples all clearly fall within the broad category of "information," and they relate to "identifiable" individuals.

19. Given the manner in which the information is stored on the relevant databases (the National DNA Database, the Police National Computer and the National Automated Fingerprint Service) and the attached biographical information the DNA profiles and fingerprints (but not the samples) also relate to "identified" individuals (indeed, if they did not do so the entire basis of the Respondent Government's support for the PACE scheme would fall).

20. In the case of the samples, in the initial collection process the Applicants' personal characteristics were captured and transformed into data, and this resulting data is personal data within the meaning of Convention No. 108: *Amann v. Switzerland,* App. No. 27798/95, ECHR 2000-II. In any event, the sample itself (hair or saliva) is a form of raw data which enables others to distinguish and identify an individual, albeit that this cannot be done by "the untutored eye" (per Lord Steyn in the House of Lords proceedings).

21. So far as the case of *Van der Velden v. Netherlands*, App. No. 29514/05, is concerned the important passage is on page 9. The case concerned a convicted person who argued that retention of DNA was an unjustified breach of Art 8 because the detection of none of his crimes would have been assisted by DNA data. The Court said, in rejecting the application that

> As regards the retention of the cellular material and the subsequently compiled DNA profile, the Court observes that the former Commission held that fingerprints did not contain any subjective appreciations which might need refuting, and concluded that the retention of that material did not constitute an interference with private life (see *Kinnunen v. Finland*, no. 24950/94, Commission decision of 15 May 1996). While a similar reasoning may currently also apply to the retention of cellular material and DNA profiles, **the Court nevertheless considers that, given the use to which cellular material in particular could conceivably**

> **be put in the future, the systematic retention of that material goes beyond the scope of neutral identifying features such as fingerprints, and is sufficiently intrusive to constitute an interference with the right to respect for private life set out in Article 8 § 1 of the Convention.** (emphasis added).

22. Thus the Court is specifically identifying possible future use of samples and profiles as the main factor for differentiating between these and fingerprints, thus placing the retention of DNA samples and profiles in a category that constitutes a breach of Art 8(1). It is submitted that the Court should follow this lead and find that retention of DNA profiles and samples, because of the future use to which they might be put, is an interference with Art 8(1) rights. However, the Applicants also reiterate their earlier submissions that Art. 8(1) readily applies to the retention of samples in particular due to the highly intimate nature of the information which they may reveal about the Applicants and their families.

23. In relation to fingerprints, the Applicants accept that the Court has drawn a distinction between fingerprints and biological material and DNA profiles in *Van der Velden v. Netherlands*, on the basis that fingerprints have "neutral identifying features" only. The Applicants submit that, although fingerprints are not as information-rich as either profiles or samples, they nevertheless retain an Article 8(1) interest in the informational component derived from their fingerprints. They rely on the prevailing practice in other European and common law countries of destroying or returning an individual's fingerprints upon acquittal or withdrawal of charges as suggesting that such a privacy interest may remain when a person is effectively cleared of the offence for which the fingerprints were taken; they also rely on the Canadian jurisprudence concerning retention of fingerprints.[3]

[3] See further Dr. Gallagher's summary at paras. 250 – 256 of her statement.

If [retention involves an interference with Art 8(1) rights] as regards (a) fingerprints (b) DNA profiles (c) DNA samples, is their continued retention justified in terms of the second paragraph of Article 8 of the Convention.

24. Again, this is a point that has been addressed at length in previous documents lodged in support of this application. However, the Court has raised a number of additional areas which are addressed in this submission.

(a) Recommendation R (92) 1

25. The Court asks whether retention can be regarded as necessary and proportionate in respect of individuals who have not been convicted of a serious crime, and refers to Recommendation No (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system (adopted on 10 February 1992).

26. The background to the adoption of this Recommendation is set out in the Explanatory Memorandum of the same date:

> The Council of Europe has interested itself for a number of years in the impact of new technologies on matters relating to human rights and fundamental freedoms. It has done so in the belief that, on the one hand, the evolution and use of these new technologies are necessary and justified in the interest of the progress of society but, on the other hand, that the use of such technologies **sometimes carries an inherent risk of infringing human rights and fundamental freedoms if the proper balance is not struck between opposite interests in accordance with what is necessary in a democratic society.** (emphasis added)

27. The Recommendation of the Council of Ministers was made having regard to the Human Rights Convention and the Data Protection Convention (see Preamble), and states that the Council of Ministers is

> Mindful however that the introduction and use of these techniques should take full account of and not contravene such

fundamental principles as the inherent dignity of the individual and the respect for the human body, the rights of the defence and the principle of proportionality in the carrying out of criminal justice .

28. Paragraphs 3, 4 and 8 are set out in the admissibility decision and are not reproduced here. Paragraph 7 reads

> **7. Data protection**
> The collection of samples and the use of DNA analysis must be in conformity with the Council of Europe's standards of data protection as laid down in the Data Protection Convention No 108 and the Recommendations on data protection and in particular Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

29. In so far as the collection of the information is concerned, reference is made to Principle No. 2 in Recommendation No. R (87) 15 regulating the use of personal data in the police sector. This principle requires that the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a criminal offence. Any exception to this provision should be the subject of specific national legislation. This principle excludes an open-ended, indiscriminate collection of data by the police. "Real danger" is to be understood as not being restricted to a specific offence or offender but includes any circumstance where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities.

30. The following points are made on behalf of the applicants

(a) Council of Ministers recommends that the governments of member States be guided in their legislation and policy by the principles and recommendations in R (92) 1.
(b) The UK has not reserved any right not to comply with any part of the Recommendation (other countries have reserved such right).

(c) Paragraph 3 states that DNA samples collected for the purpose of the investigation and prosecution of criminal offences "must not be used for other purposes".

(d) Paragraph 4 states that samples must be taken without consent only "if the circumstances of the case warrant such action". It is noted that PACE does not contain any such "individual consideration" provision for taking of DNA samples;

(e) Paragraph 6 requires, amongst other things "adequate safeguards to ensure absolute confidentiality in respect of the identification of the person to whom the result of the DNA analysis relates".

(f) Paragraph 8 in part states that "Samples or other body tissues taken from individuals for DNA analysis should not be kept after the rendering of the final decision in the case for which they were used, unless it is necessary for purposes directly linked to those for which they were collected".

(g) Paragraph 8 further states that "Measures should be taken to ensure that the results of DNA analysis and the information so derived is deleted when it is no longer necessary to keep it for the purposes for which it was used".

(h) Again further paragraph 8 states that "The results of DNA analysis and the information so derived may however be retained where the individual concerned has been convicted of serious offences against the life, integrity and security of persons"

(i) In such circumstances, "strict storage periods should be defined by domestic law".

(j) Paragraph 8 concludes by setting out different rules where the security of the State is involved, whence " the domestic law of the member State may permit retention of the samples, the results of DNA analysis and the information so derived even though the individual concerned has not been charged or convicted of an offence. In such cases strict storage periods should be defined by domestic law".

31. It is noted that in the present case almost all the recommendations in paragraph 8 have not been complied with. The Applicants' samples and profiles have been kept after criminal proceedings involving relatively minor offences have come to an end for which they have not been convicted. No measures have been taken to delete samples and profiles and there are no strict storage periods. Paragraph 8 has been drafted with the Human Rights Convention in mind. All these factors indicate an unjustified interference with Art. 8 rights, primarily on the basis that the interference is disproportionate and not necessary in a democratic society. The explanatory memorandum to paragraph 8 supports this approach

> The working party was well aware that the drafting of Recommendation 8 was a delicate matter, involving different protected interests of a very difficult nature. It was necessary to strike the right balance between these interests. Both the European Convention on Human Rights and the Data Protection Convention provide exceptions for the interests of the suppression of criminal offences and the protection of the rights and freedoms of third parties. However, the exceptions are only allowed to the extent that they are compatible with what is necessary in a democratic society.

32. However, the explanatory memorandum also explains circumstances in which the general rule that DNA material should be deleted after a case has been completed (para. 50)

> However, the working party recognised that there was a need to set up data bases in certain cases and for specific categories of offences which could be considered to constitute circumstances warranting another solution, because of the seriousness of the offences. **The working party came to this conclusion after a thorough analysis of the relevant provisions in the European Convention on Human Rights, the Data Protection Convention and other legal instruments drafted within the framework of the Council of Europe.** In addition, the working party took into consideration that all member states keep a criminal record and that such record may be used for the purposes of the criminal justice system (see Recommendation No. R (84) 10 on the criminal record and rehabilitation of convicted persons). It took into account that such an exception would be permissible under certain strict conditions:

- when there has been a conviction;
- when the conviction concerns a serious offence committed against the life, integrity and security of a person;
- the storage period is limited strictly;
- the storage is defined and regulated by law;
- the storage is subject to control by Parliament or an independent supervisory body.

33. Although of course this cannot bind the Court, the fact that the Council of Ministers came to these conclusions "after a thorough analysis of the relevant provisions in the European Convention on Human Rights, the Data Protection Convention and other legal instruments drafted within the framework of the Council of Europe" should give them great weight and the Court should be slow to reach different conclusions and/or adopt a different approach.

(b) Comparative Position

34. In relation to the question of necessity and proportionality, the Court has asked the parties to consider whether it is "relevant that the approach in the United Kingdom differs significantly from other European and international jurisdictions". The Applicants submit that the comparative position is highly relevant to questions of necessity and proportionality under Art. 8(2). The Court has on many occasions examined the situation within and outside the Contracting State in question in order to assess "in the light of present-day conditions" what constitutes the appropriate interpretation and application of the Convention (*Tyrer v. UK,* judgment of 25 April 1978, Series A no. 26, para. 31; *Goodwin v. UK* [GC], para. 75; *Hirst v. UK* [GC]).

35. It is submitted that the Respondent Government's approach is substantially at odds with that adopted by all other Contracting States

of the Council of Europe and other common law jurisdictions internationally (in particular, Canada, New Zealand and Australia). The comparative material detailed in Dr. Gallagher's statement demonstrates that the approach of the United Kingdom is grossly out of kilter with the international position.

36. Further, in relation to genetic databases, even within the United Kingdom itself England and Wales goes far further than Scotland or Northern Ireland.

DNA Profiles

37. The National DNA Database (NDNAD) of England and Wales is the largest in the world. At the end of January 2007 it contained over 3.8 million profiles. The NDNAD dwarfs other genetic databases in countries with similar populations (such as Germany) and those with significantly larger populations (such as the US). It is the largest database of its kind worldwide in both relative terms and absolute terms.

38. Its closest rival internationally is the US database, CODIS. However, over 5.2% of the population of England and Wales is included on the database, compared to 0.5% of the US population.

39. Within Europe, the closest national DNA database in size terms is that of Germany. However, the differential is huge, with Germany's database consisting of only 380,000 profiles, in contrast to the vast NDNAD of England and Wales. The third largest European database is that of Austria.

40. The NDNAD is unique internationally in retaining DNA profiles of individuals who have been acquitted in court (since 2001) and those of individuals who have previously been arrested on suspicion of a "recordable offence" (since April 2004). These individuals may have

never been charged, let alone convicted. No other national database worldwide adopts such a system.

Samples

41. The Applicants submit that the United Kingdom is unique in routinely retaining, on a permanent basis, the biological samples of individuals whose profiles have been loaded onto the NDNAD.

Collection

42. Within the Council of Europe countries assessed by Dr. Gallagher, samples are almost invariably only taken from individuals suspected of committing serious offences: Austria (dangerous assaults), Belgium (serious crimes – mainly sexual assaults and murder), France (mainly serious crimes against the person and sexual assaults), the Netherlands (offences carrying sentences exceeding 4 years), Norway (sexual abuse, crimes against life and health and crimes posing danger to the public), and Sweden (offences carrying sentences exceeding 2 years).

Retention

43. England and Wales is unique internationally in retaining, on a permanent basis, biological information and DNA profiles relating to individuals who have never been convicted of an offence.

44. Within the Council of Europe, the duration of storage of DNA samples and profiles on databases varies from country to country. Findings from the research indicate that almost every country will immediately remove an individual from their database if they are acquitted of an offence. The exceptions to this are Finland (who remove an individual from their database 1 year after acquittal), Denmark (removal after 10 years if acquitted), Switzerland (who remove an individual after 5 years if acquitted) and the UK (who will never remove an individual from its database if acquitted).

45. Even in Scotland DNA samples and profiles are only retained when someone has been convicted of a recordable offence – otherwise they are destroyed.

46. Countries such as Austria, Finland and the Netherlands also have procedures to remove an individual from their databases after a specified period of time, even after they have been convicted of a sufficiently serious offence to warrant entry on their database in the first place.

47. Within the common law jurisdictions, material relating to unconvicted individuals is not retained.

48. In Canada, although a sample can be seized from a person suspected of having committed a 'designated offence' in strictly defined circumstances, s. 487.09 of the Criminal Code provides that both the samples and the profiles must be destroyed without delay:

    (a) If the results are negative;
    (b) If the person is acquitted;
    (c) If the person is otherwise not convicted (through being discharged, dismissal other than acquittal, stay etc.) within one year, unless during that year a new information is laid or an indictment is preferred charging the person with the designated offence.

Fingerprints

49. Unlike DNA databases, fingerprint databases are commonplace in European jurisdictions. However, England and Wales is unusual in retaining fingerprint information following the acquittal or the dropping of charges against a suspect, and NAFIS is also a far larger system than any other European fingerprint database system.

50. The largest fingerprint database in the world, in absolute terms, operates in the United States (the Automated Fingerprint Identification System operated by the Forensic Sciences Division of the Secret Service). It contains over 30 million fingerprints. However, in relative terms the NAFIS system of England and Wales surpasses the size of the US system. Both the US and NAFIS systems are out of step (in absolute and relative volume terms) with other common law countries.

51. As detailed in Dr. Gallagher's statement, all common law countries reviewed do operate fingerprint database systems. In most common law countries fingerprints are routinely taken upon arrest (Ireland, New Zealand, most US states). However, it is routine for those prints to be destroyed if the individual is not subsequently convicted of a crime.

(c) Use of Samples

52. The Court has asked what is the current use of DNA samples and does this render their retention necessary for the prevention of crime and disorder. This point is addressed in this section but reference is also made to the next section on safeguards.

53. The NDNAD contains only DNA profiles, numerical representations of selected regions of an individual's DNA sequence. The original samples provided by the Applicants do not appear on the National DNA Database.

54. As detailed in Dr. Gallagher's statement (paras. 48 – 63), the sample is never relied upon for general forensic purposes following the original generation of the DNA profile. The DNA profile is loaded onto the database and remains there permanently. If there is a match between a future scene of crime sample and a profile on the NDNAD, the original sample is not used; the individual is contacted and a fresh sample obtained under PACE powers.

55. At para. 67 of the United Kingdom Government's Written Observations on Admissibility and Merits it is indicated that samples (as well as DNA profiles and fingerprints) are put to "use for checks of identity" but this is factually incorrect. In the Divisional Court and Court of Appeal it was stated that it is "essential to have some sample with which to compare the retained data" (para. 19, Divisional Court; para. 33, Court of Appeal). This is incorrect. It is not essential to have some sample with which to compare the retained data: the retained data (the profile) is *not* compared to the retained sample. There appears to have been a misunderstanding in the domestic courts of the system's operation in practice.

56. Given that the sample tends not to be subsequently used following the generation of the DNA profile, the purpose behind retention of those samples was never clarified by the domestic courts.

57. The United Kingdom Government now deals with the purpose of sample retention at para. 108 of their Written Observations on Admissibility and Merits:

> "…The samples are primarily used to generate the DNA profile from non-coded elements of DNA. The sample (be it hair or tissue) is then retained only to ensure the integrity and future utility of the DNA database system… and the DNA profile it has generated."

58. The Government has thus indicated that there are two purposes for sample retention:

(i) "to ensure the integrity and future utility of the DNA database system"; and

(ii) "to ensure the integrity and future utility" of "the DNA profile [the sample] has generated".

59. It is submitted that these vague, generalised statements of purpose simply cannot support the Government's contention that permanent retention of the samples is necessary in a democratic society and proportionate.

60. On purported purpose (ii) ("to ensure the integrity and future utility" of the DNA profile), no evidence has been advanced by the United Kingdom Government indicating how retention of the original samples after the cessation of criminal proceedings against an individual assists with maintaining the integrity of the DNA profile generated from his sample. Dr. Bramley's Witness Statement does set out details of the 'quality assurance' process (paras. 10.3, 10.8, 10.9) but this focuses on the testing of sub-samples while the original criminal investigation is ongoing in order to ensure that the correct person has been arrested or charged and does not go to the question of retention after proceedings have been discontinued.

61. On purported purpose (i) ("to ensure the integrity and future utility of the DNA database system") no detail has been provided by the United Kingdom Government in their Written Observations. However, it may be inferred from the Witness Statement of Dr. Bramley (paras. 10.3 – 10.14) that there are two possible justifications advanced by the Government. First, Dr. Bramley suggests that, in the future, it may be decided that there should be 'platform upgrade' of the system. Second, he suggests that retention of samples allows for subsequent miscarriage of justice investigations.

Platform Upgrade

62. The idea of platform upgrade is that, in future, DNA profiles could become more honed and targeted, generated using more than the current 10 STR loci. Were this possible future 'platform upgrade' to apply retrospectively, to those DNA profiles already loaded onto the

NDNAD, the argument sometimes advanced is that it would be more efficient to simply retest the original samples and include additional loci. This approach is implicit in the statement of Dr. Bramley but has not been fully detailed by the Respondent Government in its submissions to the Court.

63. The Applicants submit that this is purely hypothetical, a speculative assessment of possible future developments in DNA profile generation. A speculative, hypothetical argument in favour of retention of biological material containing the Applicants' full genetic sequences cannot, it is submitted, satisfy the twin requirements of necessity and proportionality. The Respondent Government itself at para. 108 of its Written Observations urges the Court to judge Article 8's application "against the present rather than against a theoretical future".

Miscarriages of Justice

64. Dr. Bramley suggests (para. 10.13) that retention of samples may be useful for the investigation of alleged miscarriages of justice. This point was noted by the domestic courts. DNA evidence is, indeed, a powerful tool, and it is capable of ruling an individual *out* of involvement in a crime with more certainty than it can rule an individual *in*: see also the Explanatory Memorandum to Recommendation R (92) 1, paras. 1, 2.) However, this does not justify retention of such information indefinitely.

65. First, in the vast majority of cases involving an alleged miscarriage of justice the aggrieved party will be willing to provide a fresh sample for reanalysis. It is difficult to see how the 'exculpatory' argument can justify the retention of personal information on various databases on a permanent basis, when the individual suspected would be ruled out of involvement immediately upon providing the sample he is required to give post-arrest under PACE.

66. Second, if an individual is suspected of involvement in a crime, under PACE powers he is required to, with or without consent, give a DNA sample to the police, and a DNA profile will be generated from that sample and compared to the profile from the scene of crime sample in question. If the individual has no involvement in that crime, his fresh sample will prove this.

(d) Safeguards

67. The Court has asked what procedural safeguards exist which regulate, with due regard to the interests of confidentiality and protection of personal data, access of others to the materials/information, the use to which the material/ information is put and the length of time over which retention is possible? Is there any independent oversight of the functioning of the DNA database?

68. Some of these points have already been addressed in the previous documents filed in support of this application. Dr Gallagher's statement also contains a detailed description as to how the system "works" including a detailed analysis of the safeguards that exist: see Sections B and C of her statement (paragraphs 4-128).

69. This section also deals with the comparative aspects of safeguards and use.

<u>Safeguards in the UK</u>

70. It is widely regarded by countries with DNA databases that safeguards are essential to protect the information contained in both DNA profiles and samples. Samples are highly sensitive and capable of revealing an individual's complete genetic make-up. Although profiles are generated from a limited number of short tandem repeats "STRs", and

although they reveal less information than the original sample, there are already known associations with the information in profiles and schizophrenia, susceptibility to Down's Syndrome and ethnic origin. (*Witness Statement of Eric Downham at paragraph 49*).

71. It is accepted by the UK government that a system of safeguards is necessary. However the current system is insufficient given the privacy implications of the information contained in samples and profiles.

72. The statutory basis for the storage of samples and profiles is contained in section 64 PACE, which only limits the use of profiles to "purposes related to the prevention or detection of crime"; "the investigation of an offence"; "the conduct of a prosecution"; or "the identification of a deceased person or of the person from whom the body part came". These uses are vague and broad in their scope. There is no definition of the purposes "*related to* the prevention or detection of crime", which could include intelligence gathering and other forms of collation of detailed personal information, outside the immediate context of the investigation of a particular offence.

73. While other countries have separate and specific safeguards for samples and profiles, in the UK there is no statutory distinction between samples and profiles. The only distinction in the UK law is that between "intimate" and "non-intimate" samples (ss62 and 63 PACE with Code D), which fails to take into account the fact that the *taking* of a sample by non-intimate means (eg. a mouth swab) is capable of revealing their complete genetic make-up and hence the most intimate biological data available.

74. Profiles are stored on the DNA database with the name, date of birth, sex, ethnic appearance and offence type for which the DNA sample was taken. The record on the NDNAD also includes what is known as the "Phoenix Arrest/ Summons report number" which provides a link between the NDNAD and the Police National Computer ("PNC").

75. Information is available through the PNC which is accessible through more than 10,000 computer terminals nationwide to 56 bodies, including governmental intelligence agencies and the secret service, government departments and groups such as the Association of British Insurers. Other third parties may demand access to PNC records using the practice of 'enforced subject access' described (*Mr. David Smith, Assistant Commissioner, Information Commissioner's Office at p. 3 of document CG 1*). So far no measures have been taken to restrict these records to police users only.

76. The Information Commissioner's Office has recommended that information retained on the PNC should be limited to identification details such as height or eye colour, rather than containing details of the alleged offence. It has further recommended that records which would not in themselves be retained on the PNC should be stripped down to the bare identifiers, and also be "removed from the main system and held in such a way that it could only be accessed by means of a DNA profile" (*Mr. David Smith, Assistant Commissioner, Information Commissioner's Office at pp. 2-3 of document CG 1.* This, and other minimum safeguards recommended by the Commissioner, were not implemented. (*Witness Statement of Dr Caoilfhionn Gallagher at paragraph 91*).

77. There is no separation of databases as between samples taken by police of suspects, crime scene samples, volunteers (who have been incorporated since August 2004 – before that they had a separate database). The information and links detailed above therefore provide that information about individuals who have never been suspected of a crime are available alongside those suspected and those convicted.

78. Samples are not held by a central laboratory but by the Forensic Science Service and Supplier Laboratories. There are no specific requirements governing these sample banks except that they be kept at

-15^{0}C and meet the international quality standard and the Data Protection Act 1998.

79. The National DNA Database is overseen by a Board composed of the Home Office, the Association of Chief Police Officers and the Association of Police Authorities. The Human Genetics Commission ("HGC") are also represented, although they have raised concerns that their representation is not an adequate substitute to a National Ethical Committee. The Home Office published an advertisement in the *The Times* newspaper on Tuesday 13th March 2007 advertising positions for a Chair and up to 8 members of the 'Ethics Group of the National DNA Database' confirming that no such group as yet exists despite the fact that "Independent ethical advice and input is necessary to ensure that appropriate account of a wide set of views, and protection of individuals rights, is retained in the decision-making process". (*The Times*, *13th March 2007*).

80. The consequences of failures in the current system of safeguards and ethical scrutiny in the UK have already become apparent. Five research proposals were submitted to the Board since 1995, 2 of which related to ethnic and familiar traits; these were granted with on requirement of consent from the individuals. In May 2004 a prosecution error led to a man discovering that he was HIV positive as he stood in a witness box in a court in Leicester 'Witness told in court he has HIV,' *The Guardian*, 25th May 2004, and CG8, 'Inquiry into HIV court blunder,' *BBC News*, 25th May 2004).

81. There are no specified penalties or criminal sanctions in the UK for breach of the permissible uses of samples and profiles.

Comparative Analysis of Safeguards Governing DNA Databases

82. The inadequacy of the UK system is clearly revealed by a comparative analysis of safeguards. Not only have other jurisdictions introduced

rigorous regimes safeguarding DNA data banks and sample storage, but it is these safeguards that have been held fundamental by courts considering whether the retention of samples and profiles is a justifiable infringement of privacy.

Canada

83. In Canada as in the UK both the profiles and the samples of convicted offenders are retained. Unlike the UK where disparate laboratories host samples, in Canada they are stored in the national DNA data bank. Although they may be used for further forensic analysis in the future, this is conditional upon "significant technological advances" and their being subject to the same rigid controls as applies to the current profile and sample regime. *Section 10 DNA Identification Act ("DNAIA").* The importance of these controls is emphasized by section 4(c) of the *DNAIA* which sets out the need to respect the privacy of individuals and places safeguards on the use and communication of samples and profiles.

84. Whereas in the UK profiles are stored with personal information relating to the individual, such as name, date of birth, sex, ethnic appearance and offence type, in Canada profiles are stored with only a unique identification number; the identification of the donor is then removed. The identification of the profile with the donor is linked by a bar code, which is not accessible to data bank staff. Similar safeguards recommended for the UK system by the Information Commissioner have so far not been implemented.

85. The circumstances under which this information can be communicated is defined by statute (*section 6 DNAIA*). Contrary to the vague purposes for which DNA profiles can be used in the UK under s64(1A) PACE, in Canada they are only accessible for "forensic analysis" which is defined in the Canadian *Criminal Code* as "comparison of DNA from sample with results of DNA from crime scene sample" (*s 487.08(1)*).

86. Prior judicial authorization is required DNA samples to be obtained. Under section 487.05 of the *Criminal Code*; the judge must have reasonable grounds to believe an offence has been committed, DNA evidence exists, and that the suspect was a person party to that offence. The judge must have regard to all relevant matters, including (but not limited to) the nature of the designated offence and the circumstances of its commission and be satisfied that it is in the best interests of justice to do so (*section 487.05(2)(a) Canadian Criminal Code*).

87. Not only are the uses of DNA clearly defined in Canadian law, but anyone in breach of those statutory provisions for accessing profiles faces criminal liability and a maximum penalty of two years imprisonment (*sections 6(6), 6(7), 8, 10(3), 10(5), 11, DNAIA*). It is a further criminal offence to use bodily samples or results of forensic DNA analysis obtained under a DNA data bank authorization other than for transmission to the national DNA data bank. A breach of that provision is a hybrid offence that when prosecuted by indictment is subject to a maximum penalty of two years imprisonment: (*sections. 487.08(2) and (3) Criminal Code.*

88. Canadian Supreme Court authority has held the existence of these safeguards fundamental in its findings that that retention of DNA was a justified infringement of privacy. *R v S.A.B* [2003] 2 S.C.R. 678, 2003 SCC 60, per Arbour J at para 4; *R v Rodgers* [2006] 1 S.C.R. 554, 2006 SCC 15, per Charron J at para 11.

United States

89. The U.S. "Combined DNA Index Systems Database" ("CODIS") has allowed for the storage of DNA profiles from both convicted offenders and suspects since 2004 (*Justice for All Act 2004*). There are no uniform provisions to this end and each state has a different legislative scheme governing the use and retention of samples and profiles.

90. Challenges to some of these provisions under the Fourth Amendment have led to the finding that DNA seizure from a suspect is only justified pursuant to a judicial warrant establishing probable cause. *Kohler v. Englade, U.S Court of Appeal Fifth Circuit, No. 05 -30541 the Fifth Circuit Court of Appeal found on 21st November 2006*, a decision in line with the requirements in Canada, for example.

91. California, the largest state in the U.S. with a population of over 30 million, has similar provisions to the UK for the taking and retention of samples from suspects as well as convicted offenders. However unlike the current UK system in California this is combined with provisions for the "expungement" of both the profile and sample on written request where there is no ultimate conviction (*California Penal Code § 299(b)(2005)*. New Jersey, the 10th largest state in the US with a population of over 8 million, has a similar requirement that DNA samples and profiles from convicted persons must be purged from the system at the request of an ex-felon who has "fully resumed civilian life". *A.A. v Attorney General, No. MER-L-034604* (N.J. Super.Ct.Law.Div.2004) (p. 230), *per Judge Sabatino. Superior Court of New Jersey for Mercer County at 2-3.*

Australia

92. A national DNA Database has been established in Australia but is currently still operating according to the provisions of each State Territory. Victoria, the second most populous state in Australia with a population of around 5 million, deliberately adopted a more restricted and carefully safeguarded regime than that in the UK, having conducted a comprehensive comparative review (*The Victoria Parliament Law Reform Committee, Forensic Sampling and DNA Databases in Criminal Investigations (Melbourne VPLRC, 2004). (p. 230)*.

93. Under Victorian law, samples are obtained from suspects as well as from convicted offenders. However in contrast to the UK where there is a power to take samples from all suspects and arrestees, in Victoria this only applies to suspects of a narrow range of offences, all of which are serious and / or violent crimes. A judicial warrant must also be obtained. This system, which was regarded by the Victoria Parliament Law Reform Commission as having substantial privacy implications, is justified by the fact that both samples and profiles are only retained from suspects for a period of 12 months. In the UK, which does not have even Victoria's initial safeguards, there is no such provision.

Germany

94. Whereas samples are retained indefinitely in the UK after profiles have been generated from them, in Germany they are destroyed as soon as no longer required for criminal proceedings (s81(a) *German Criminal Procedure Code ("StPO",*). Profiles are only retained for convicted offenders and these are checked every 10 years for an adult and every 5 years for a child as to whether still relevant.

95. In contrast to the widespread access to profiles in the UK through the PNC, in Germany only "Landeskriminalämter" – Federal State Investigators, and not ordinary police forces, have access to the profiles. The purpose for which they can be accessed is defined by statute as confined to criminal proceedings, averting danger, or providing international legal assistance (*s3, DNA-Identitätsfestullungsgesetz 1998*).

96. Prior judicial authorization must be obtained before profiles can be used. (s81f *StPO*). An individual also has a right of appeal against any such authorization. It was on the basis of these controls that the infringement of Article 8 in retaining profiles was held to be justified by the German Constitutional Court ("Bundesverfassungsgericht") in

the cases 2 BvR 1741/99 (2000) and 2 BvR 1841/00 (2001). There is no equivalent to either of these provisions in the UK.

Netherlands

97. Whereas samples can be taken from any arrestee in the UK, in the Netherlands not only must an individual have been convicted, but his offence must carry a statutory maximum prison sentence of at least four years (s. 2(1) *DNA Testing (Convicted Persons) Act* ("*Wet DNA-onderzoek bij veroordeelden"*)). This is not a blanket provision but is exempted where it may reasonably be assumed that the determination and processing of the DNA profile will not be of significance for the prevention, detection, prosecution and trial the offences in question The purposes for which DNA profiles can be used is strictly limited to the prevention, detection and prosecution and trial of criminal offences: (*section. 2(5) DNA Testing (Convicted Persons) Act.*).

98. Dutch law also limits the duration for which DNA samples and profiles can be retained. The period is 30 years if the offence carries a statutory sentence of 6 years or more, and 20 years where the sentence is up to 6 years - *DNA (Criminal Cases) Tests Decree ("Besluit DNA-ondersoek in strafzaken").*

99. As in Canada and Germany where an individual has a right of appeal, in the Netherlands an individual must be notified that DNA material is to be taken for a profile, and may lodge an objection with Regional Court within 14 days: *section. 2(5) DNA Testing (Convicted Persons) Act.*).

Conclusion

100. Both the retention and use of the fingerprints, DNA profiles and DNA samples of innocent persons, which PACE now allows, is a

significant interference with the rights of such individuals under Article 8(1) of the European Convention on Human Rights. The information gathered and retained is far more intimate and intrusive than was recognised by the domestic courts; the creation of a record on the PNC, and resulting access to that record by a wide range of public authorities for a wide range of purposes, was not understood in the domestic courts; and the domestic courts failed to appreciate the distinction between DNA samples and DNA profiles.

101. Retention of such information is a fresh invasion of Art. 8 ECHR interests and must be subjected to fresh Art. 8(2) analysis. The Canadian approach to s. 8 of the Charter (the protective mantle only applies while the original justification for the taking of the material is still active) and the German Constitutional Court approach, applying proportionality analysis to each separate privacy invasion, are to be preferred over the approach of the domestic courts in *S and Marper*.

102. The interference in this case is not justified under Article 8(2) of the Convention because it is disproportionate to the legitimate aims being pursued. R (92) 1 and its explanatory memorandum (as analysed above) support this submission.

103. In addition, even if the Court accepts the government's claim that there are legitimate reasons for retention, the state must also justify rejecting the available 'less restrictive means' of achieving that objective, in particular the more privacy-friendly systems proposed by the Information Commissioner's Office (see exhibit).

104. In assessing whether the UK's approach is within its 'margin of appreciation' regard should be had to the fact that the UK's approach to both DNA databases and fingerprint databases is far more intrusive than that of any other Council of Europe or common law country worldwide. The UK is severely out of kilter with the approach in other democratic systems. Within Europe, the NDNAD of England and

Wales is 800% larger than its closest rival in size, Germany's national database.

105. Not only does no other country in the world have a database on the scale of NDNAD or NAFIS, neither does any other country in the world treat its innocent citizens who have previously been incorrectly suspected of involvement in an offence en masse in the same manner as its convicted criminals. Further, the NDNAD and NAFIS have fewer safeguards than other large systems, and the NDNAD does not have an independent custodian monitoring its use and access to the sensitive information it contains.

106. At the very least, the keeping of DNA samples is unjustified. As they are not currently used for forensic purposes no legitimate purpose is pursued by their retention. Other countries with forensic DNA identification systems either destroy the sample immediately once the profile has been generated (New Zealand, Germany, Sweden, Denmark, the Netherlands) or permit the destruction of the sample at an earlier stage than the destruction of the profile or fingerprint (Australia). No other system worldwide retains DNA samples indefinitely. These systems recognise that the information contained in a DNA sample differs markedly from that contained in a DNA profile or fingerprint.

107. The blanket, permanent retention and open-ended use of personal information through the NDNAD, NAFIS and PNC under the PACE regime is unacceptable, and places the applicants at a permanent disadvantage when compared to those who have never been arrested (not on the relevant databases) and the police themselves (on an alternative database for a limited period of time, and with strong safeguards). It equalises the applicants with convicted criminals and, despite official assurances to the contrary, continues to mark them with the taint of criminality.

108. For the reasons set out above, it is submitted that this application should be allowed and the Court should declare a violation of Article 8 and Article 14 of the Convention.

Just satisfaction

109. The Court has asked the Applicants to address the issue of "just satisfaction" under Art 41 of the Convention. The Applicants do not claim any pecuniary damages in relation to the claimed violations of the Convention.

110. The Applicants do claim non-pecuniary loss in the form of distress and anxiety caused by the knowledge that intimate information and material about each of them has been unjustifiably retained by the State, as expressed in their statements for the domestic court hearing. The Applicants also claim such damages in relation to the anxiety and stress caused by the need to pursue this matter through four levels of court, including the House of Lords and this Court. Nevertheless, the Applicants limit their claim to £5,000 each. The Applicants also claim the costs and expenses linked with pursuing this important matter through the domestic courts and to this Court, and enclose the documentation to support this aspect of the claim.

RICHARD GORDON QC

STEPHEN CRAGG

PETER MAHY

15 March 2007