IN THE EUROPEAN COURT OF
HUMAN RIGHTS **C.**
Gallagher

Witness
Statement

APPLICATION NOS. 30562/04 30566/04
March 2007

(1) 'S'
(2) MARPER

V

THE UNITED KINGDOM

WITNESS STATEMENT OF DR. CAOILFHIONN GALLAGHER

TABLE OF CONTENTS

A. INTRODUCTION

1. My full name is Caoilfhionn Anna Gallagher. I am registered as a Council of Europe expert on Articles 8, 10 and 11 of the European Convention on Human Rights (ECHR), and I have co-authored one of the leading texts on the Human Rights Act, *Blackstone's Guide to the Human Rights Act 1998*, 4th edn (Oxford: Oxford University Press, 2007). I have specialised in comparative privacy law generally and Article 8 of the European Convention on Human Rights (ECHR) in particular for 8 years.

2. I am a barrister in two Council of Europe jurisdictions (Ireland, and England and Wales) and currently practice from London. In 2005 I was the Policy Officer for Liberty (the National Council of Civil Liberties).

B. HOW THE FORENSIC IDENTIFICATION SYSTEM OF ENGLAND AND WALES OPERATES

I Types of Material at Issue in this Case

3. At issue in this case are three different types of material: (a) samples, (b) DNA profiles and (c) fingerprints. Each is considered in turn below. Each is capable of performing an identificatory function, but (a) and, to a more limited extent, (b), also reveal a range of non-identification information about the person to whom they relate.

(a) Samples

4. Samples are the original bodily material provided by a suspect or a volunteer during a criminal investigation. The samples are usually cells taken from the inner cheek, but can also consist of hairs and blood samples.

5. All of the DNA in an individual is formed through the duplication of the DNA from a single cell, and therefore DNA in different body fluids from the same person will be the same in all but the rarest of cases.

6. DNA is found in almost every cell in the body. It is arranged into chromosomes and is inherited from both parents, so 50% of a child's DNA comes from its mother and 50% from its father. This trait of inheritance means that examining two DNA samples from apparent relatives (father and daughter, for example) can reveal whether the two individuals are, in fact, related, and so can reveal 'false paternity'.

7. DNA samples are capable of revealing highly sensitive, intimate information about the individual and his family, such as the person's genetic susceptibility or predisposition to particular genetic disorders, and his status as a 'carrier' of a condition that may affect his children.

8. It is estimated that there are over 3,500 'established' and 2,500 'suspected' genetic disorders (see V.A. McKusick, *Mendelian Inheritance in Man: Catalogs of Autosomal Dominant, Autosomal Recessive and X-linked Disorders*, 11th edition, John Hopkins University Press, 1993, cited by Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms*, Cambridge University Press, 2002, p. 88). Already 95% of the most common genetic diseases can be tested for, along with several hundred rarer genetic diseases and conditions, and – as one commentator has noted – "this is likely to rise to a thousand or so more… as the human genome project bears fruit" (G. Vines, 'Gene Tests: the Parent's Dilemma,' *New Scientist*, November 1994, pp. 40-42).

9. It has been suggested that DNA samples are the 'blueprint for life' or the 'future diary' of the individual, and so genetic information is even more sensitive and private than standard medical information:

> "In privacy terms, genetic information is like medical information. But the information contained in the DNA molecule itself is more sensitive because it contains an individual's probabilistic 'future diary,' is written in a code that has only partially been broken, and contains information about an individual's parents, siblings, and children." (George J. Annas, "Privacy Rules for DNA Databanks," (1993) 270 *Journal of the American Medical Association*, pp. 2346 – 2350.)

10. Graeme Laurie, who has acted as an adviser and rapporteur on genetic databases to the World Health Organisation, describes the private nature of genetic information contained in nuclear DNA:

> "Information concerning an individual's genetic make-up is of a highly sensitive and personal nature. To discover that one is likely to develop a debilitating condition in later life or that this might be passed to one's children must be an intense and possibly devastating experience. Exposure to such knowledge can alter self-perception and challenge notions of identity, and could adversely affect an individual in her social, professional, and familial milieux. The mere availability of genetic information serves to heighten concerns about the use to which it might be put, uses which might in turn compromise the person who has been tested…
>
> Uniquely, genetic tests can also reveal information about blood relatives of the [individual], with a corresponding threat to their interests and their privacy. Family members might be loath to learn of a relative's predisposition to a particular genetic condition, given the likelihood that they carry a similar risk." (*Genetic Privacy: A Challenge to Medico-Legal Norms*, pp. 90, 91.)

11. In addition to genetic information discernible from DNA samples generally, blood samples can reveal the person's current HIV status and other such information concerning non-genetic illnesses or diseases.

(b) DNA Profiles

12. A DNA profile is generated from a DNA sample. It contains less information than the sample and is, essentially, a numerical representation on a graph of certain key information contained within the sample.

13. The focus of a DNA profile is on identifying the individual. Whilst it does contain some non-identification information, it is far more limited than tat in a DNA sample.

14. With the exception of identical twins, each person's nuclear genome (DNA within a cell's nucleus) is unique. It is also extremely large, containing around 3 billion pairs of bases, which means that all of the differences between individuals cannot be determined in a fast and cost-effective manner for forensic purposes.

15. However, research has shown that there are specific parts of a person's DNA that show limited and measurable variation. One classification of variants is termed a 'short tandem repeat' (STR). These are areas of the DNA molecule where short sequences repeat side-by-side. The number of repeats varies within a small range, and there will only be a limited number of different variants that any individual could have. By examining the DNA types at a number of different STR areas it is possible to produce a more or less discriminating 'DNA profile' that would be shared by more or less people.

16. Currently, DNA profiling in England and Wales uses ten STR areas or 'loci' and an area of DNA that determines sex. The profile consists of a series of numbers, representing the number of repeat units observed at each of the studied loci. Variation in the DNA types at one or more STR loci is sufficient to discriminate between different individuals.

17. In contrast to the ten STR areas used in England and Wales, the US uses a more discriminating technique (partly due to its far larger population) and observes 13 STR areas or loci to generate a profile.

18. DNA profiles do not reveal as much information as DNA samples, but they do reveal more than merely identification information. They may reveal gender (although this is not 100% accurate), likelihood that the individual belongs to a certain race, and likelihood that a person has

red hair, for example. As science makes it possible to identify new markers the amount of non-identification information which can be gleaned from DNA profiles is expanding.

19. DNA profiles may also reveal false paternity and kinship relationhips.

(c) Fingerprints

20. Each person's fingerprints are considered to be unique and therefore capable of identifying the person. A person's fingerprints remain unchanged for life, unless injury (burning or dermal-deep scarring) obscures or otherwise affects the pattern. An individual's fingers may all have the same pattern-type or the pattern may differ from finger to finger.

21. The skin found on the underside of the fingers, the palm, the underside of the toes and the soles of the feet differ from the rest of the skin on the human body as it possesses ridges, the raised lines that can be seen on the fingertips. A range of fingerprint pattern-types can be found, ranging from simple 'arches', 'loops' and 'whorls' to more complex patterns.

22. These 'ridge characteristic' or 'ridge patterns' of finger-, palm- and footprints are developed in the womb. Paul Bogan has described the development process as follows:

> "During the fourth week of foetal development the limb buds start to form. During the fifth week the first traces of the hands and the feet can be seen. By the eighth week the distinction between the arm and forearm, the thigh and lower leg is apparent as well as the interdigital clefts. At 10 to 11 weeks localized proliferations occur in the epidermis that eventually develop into primary ridges. Between 10 to 16 weeks the primary ridges continue to grow in an unpredictable fashion. Surface furrows begin to form. Between 16 and 24 weeks secondary ridges (also known as incipient or immature ridges) start to

> form. Various stresses cause unpredictable buckling of the ridges. No new primary ridges now form, the ridges are set for life and they continue to grow and mature." (*Identification: Investigation, Trial and Scientific Evidence*, p. 268.)

23. It is possible to compare two fingerprints (one recovered from a crime scene and one obtained from a suspected individual), identify similar features in both impressions and offer an opinion as to the likelihood of a match. This is done by an expert comparing the flow of individual ridges combined with the pattern-type, size, shape and the relationship and geography of ridge endings, convergences and divergences that individualise each finger impression.

(d) Distinctions between Samples, Profiles and Fingerprints

24. Law enforcement gathering and use of samples, DNA profiles and fingerprints are often equated, as both DNA and fingerprints are compared with evidence from a crime scene to determine whether there are identifying matching features. However, the information obtained from a DNA sample is far more extensive. According to the Human Genome Project, coordinated by the United States Department of Energy and National Institutes of Health to map and study the entire human genetic sequence:

> "DNA profiles are different from fingerprints, which are useful only for identification. DNA can provide insights into many intimate aspects of a person and their families, including susceptibility to particular diseases, legitimacy of birth, and perhaps predispositions to certain behaviours and sexual orientation. This increases the potential for genetic discrimination by government, insurers, employers, schools, banks and others." (US Department of Energy, Office of Science et al., *DNA Forensics*, Human Genome Project Information, last modified 12th January 2004.)

25. The US Human Genome Project also notes that even the DNA *profile* may provide such sensitive information, not only the DNA *sample*: "although the DNA used is considered 'junk DNA'… in the future this information may be found to reveal personal information such as susceptibilities to disease and certain behaviours" (*ibid*.).

26. A major, two-year inquiry by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council similarly found a substantial distinction between a DNA profile and a fingerprint:

> "Media and other accounts often suggest that DNA profiles are simply a modern form of fingerprint identification. In fact, DNA profiles differ from conventional fingerprints in several important respects. First, DNA holds vastly more information than fingerprints. A DNA profile can be used in establishing kinship relationships, and the sample from which the profile was obtained may hold predictive health and other information of a sensitive nature. Second, as genetic information is shared with biological relatives, an individual's profile might indirectly implicate a relative in an offence. Third, while it can be difficult to obtain fingerprints of such quality as to be useful in an investigation, DNA can be amplified from tiny and aged samples, and may be recovered from almost any cell or tissue." (Australian Law Reform Commission and Australian Health Ethics Committee, National Health and Medical Research Council, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96, 2003, attached as document CG1.)

27. The UK's Human Genetics Commission (HGC) in its 2002 Report, *Inside Information: Balancing interests in the use of personal genetic data* (attached as document CG2), noted the common confusion between DNA samples and DNA profiles:

> "It is worth noting that many responses [to the HGC's consultation] drew no distinction between the DNA profile (the numbers stored on the National DNA Database) and the original sample provided by a

> suspect or volunteer. We believe that there are important distinctions to make between these two seemingly interchangeable terms.
>
> The *DNA profile* contains a very limited amount of what we consider to be personal genetic information. With some possible minor exceptions, it does not contain any predictive information about a person's likelihood of future disease. It does, potentially, enable conclusions to be drawn about parentage or relationships, but only if it is compared to other identifiable samples. On this basis, it does not appear to constitute 'sensitive genetic information'…
>
> The *sample* on the other hand contains the full genetic information of the individual and it would be possible to derive information about that person and about others. It therefore has the potential to be used to generate personal genetic information. It should also be subject to the normal considerations of respect for persons, such as privacy and confidentiality." (pp. 146, 147, paras. 9.6, 9.7.)

28. In summary, samples contain vastly more information than DNA profiles, and, in turn, DNA profiles contain vastly more information than fingerprints. Fingerprints generate identification-related information only; DNA profiles identification-related information, kinship and paternity information, and limited ethnicity and other information (although the range of information to be gleaned from profiles is rapidly expanding); and DNA samples reveal "the full genetic information of the individual," including highly sensitive, intimate information that the individual himself may not even be aware of (e.g. current diseases or illnesses the individual has, his propensity to future diseases, and the propensity of his children to diseases).

29. It should be noted that in the case of *Murray v UK* (1994) 19 EHRR 193 the respondent state did not even dispute that its measures involving the least information-rich of these three materials, fingerprints, interfered with the respect for the rights protected under Art. 8(1) ECHR. In contrast, in the present cases in the House of Lords (*R (S) v Chief Constable of South Yorkshire* and *R (Marper) v Chief Constable of South Yorkshire* [2002] All ER (D) 367, [2002] 1 WLR 3223 and [2004] UKHL 39)) the State did dispute that Art. 8(1) even

applied to the retention of even the most information-rich of these materials, the samples.

II. Relevant Legislation

30. The taking, retention and use of fingerprints and samples, and the retention and use of DNA profiles, are governed by the Police and Criminal Evidence Act 1984 (PACE) as amended by the Criminal Justice and Police Act 2001 (CJPA) and the Criminal Justice Act 2003 (CJA). At issue in this case are the amendments made to PACE by the CJPA 2001.

31. Until CJPA 2001 an innocent individual who had given the police a DNA sample or fingerprints in connection with the investigation of a criminal offence who had been cleared of involvement in that offence or who had no criminal charges outstanding against him was entitled to have that material, any accompanying DNA profile generated from his submitted DNA sample, and any copies of his fingerprints, destroyed. He was also entitled to witness the destruction of such material, to have access to any computer data relating to the fingerprints or DNA rendered "impossible" as soon as practicable for the police to do so, and to have a certificate issued to him within three months guaranteeing that the police had complied with these statutory obligations. In other words, the innocent individual who had been wrongly suspected of involvement in an offence was entitled to be returned to the position he was in before his involvement with the police: no biological material of his was to be retained by the state, no bodily impressions (such as fingerprints) were to be retained by the state, and no police records outlining the unfounded suspicion were to be accessible.

32. Since the CJPA 2001 amendments to PACE, innocent individuals such as the Applicants are no longer returned to the position they were in

vis-à-vis the police prior to their mistaken arrests. There is now a statutory discretion to permanently retain information gathered and generated in connection with the investigation of a particular criminal offence, and to use it for unspecified purposes in the future. In practice, the statutory discretion is operating in a blanket manner, and all such information is retained and subject to future uses.

33. In the Applicants' cases, the state has refused to destroy the information gathered from them in connection with the investigation of particular offences in 2001, despite the fact that 'S' has been acquitted and the prosecution against Mr. Marper has been discontinued. The state has also refused to destroy copies of, and profiles generated from, such information. The state also continues to hold computer data relating to the Applicants which is linked to the retained materials. These materials and information will be permanently held.

34. PACE makes no distinction whatsoever between the retention of fingerprints, samples, or the identifying information derived from samples in the form of profiles, notwithstanding that the information that may be obtained from each (and therefore the "private" nature of each) may be very different. Section 64(1A) PACE does not mention DNA profiles, and instead refers to 'fingerprints or samples' in the same statutory breath. (To compound this statutory melding of the separate categories of fingerprints, samples and profiles, the domestic courts in *S and Marper* failed to distinguish between these categories in assessing proportionality under Arts. 8 and 14 ECHR. This issue is considered further at section E of this witness statement.)

35. PACE does distinguish, in another context, between different types of forensic material gathered by the police for identification purposes. PACE distinguishes between 'intimate' and 'non-intimate' samples. Police powers to obtain intimate and non-intimate samples are provided by PACE and were extended by amendments made by the Criminal Justice and Public Order Act 1994 (CJPOA). Further

guidance as to the exercise of these powers is contained within Code D of the PACE Codes of Practice. S. 65 PACE and Code D, para. 6.1, provide the definition of intimate and non-intimate samples:

> "(a) an 'intimate sample' means a dental impression or sample of blood, semen or any other tissue fluid, urine, or pubic hair, or a swab taken from a person's body orifice other than the mouth;
>
> (b) a 'non-intimate sample' means:
> (i) a sample of hair, other than pubic hair, which includes hair plucked with the root…;
> (ii) a swab taken from any part of a person's body including the mouth but not any other body orifice;
> (iii) saliva;
> (iv) a skin impression which means any record, other than a fingerprint, which is a record, in any form and produced by any method, of the skin pattern and other physical characteristics or features of the whole, or any part of, a person's foot or any other part of their body."

Section 62 PACE, with Code D, governs police powers to take intimate samples; section 63 PACE, with Code D, governs the power to take non-intimate samples. S. 62 incorporates additional safeguards (e.g. the consent of *both* the person *and* a police officer of at least the rank of inspector is needed) and stricter grounds for authorisation than s. 63, a reflection of the more invasive process involved in taking an intimate sample than a non-intimate one.

36. PACE correctly distinguishes between these categories of sample when assessing the *'taking'* process. A system which applied the same consent requirements, authorisation grounds and safeguards to the plucking of a pubic hair from an individual's genital area and the plucking of a hair from an individual's head by a police officer would assuredly cause both judicial and public concern in any democratic state. In assessing the 'taking' of samples, the physical invasiveness of the process involved is highly relevant to assessing both the extent of the Art. 8(1) right involved and the proportionality of the process under Art. 8(2) ECHR. PACE considers physical invasiveness not only

highly relevant, however, but the sole factor in categorising samples as intimate or non-intimate.

37. In contrast, PACE makes no distinction between different categories of biological material and bodily impressions, and the intimacy or sensitivity of the information generated from those materials and impressions, when considering the *'retaining'* process and subsequent *'using'* of such retained materials and impressions. I contend that when retaining such information the invasiveness of the original physical process is only one pertinent factor to be considered, and the nature of the information involved is highly relevant. PACE ignores this latter factor. There is no statutory recognition of the differing levels of informational privacy involved in DNA samples, DNA profiles and fingerprints, or the associated computer data linked to such materials. In fact, there is no fresh categorisation of materials at retention stage. A mouth swab is defined as a non-intimate sample at 'taking' stage as the mouth is not considered an intimate orifice, for example, and at no point does PACE recognise that a mouth swab is a DNA sample, capable of generating highly personal, intimate, sensitive information concerning the person's genetic make-up, relations with others and relatives' propensity to genetic illnesses. PACE's categorisations are based purely on the relative physical invasiveness, and informational invasiveness is ignored in the statutory scheme.

38. In addition to retention of DNA samples, profiles and fingerprints, PACE as amended widens the future uses that may be made of such materials. These uses are no longer limited to checks made under section 63A PACE (i.e. the "checking against other fingerprints and samples"). They now merely "include" such checks.

39. Such other uses of retained fingerprints and samples are unspecified. The only limitation is that the use that may be made of samples must fall under one of the following four heads (s.64 (1A) PACE):

(a) use for "purposes related to the prevention or detection of crime";

(b) use for "the investigation of an offence";

(c) use for "the conduct of a prosecution"; or

(d) use for "the identification of a deceased person or of the person from whom the body part came" (this last head is a recent addition to s. 64(1A), having been made by s. 117, Serious Organised Crime and Police Act 2005, and having come into force on 7th April 2005).

Categories (b) and (c) relate not only to the investigation and prosecution of the particular offence for which the material was supplied, but also future offences and prosecutions. The focus in the domestic courts in was upon category (b) but there are also concerns relating to the potentially wider and more general scope of uses for the purposes "*related to* the prevention or detection of crime". This certainly includes intelligence gathering and other forms of collation of detailed personal information, outside the immediate context of the investigation of a particular offence. It has also (as detailed later in this witness statement, section C) been interpreted in practice to allow wide-ranging research projects.

40. Two particular concerns should be noted. First, there is no detailed regulation of the particular uses that the material may be used for. Effectively, the authorities have a *carte blanche* to use the material in any way they wish provided it falls within the very broad four objectives defined by s. 64(1A) PACE. Secondly, there is no obligation to consider whether the use made of the material is proportionate whenever a particular decision is made to access and make use of the information it contains.

III. Relevant Systems

(a) National DNA Database

41. The NDNAD was established in 1995 under the custodianship of the Forensic Science Service (FSS) on behalf of the Association of Chief Police Officers (ACPO).[1] Its original primary goal was to assist the detection of serious crime suspects, relating in particular to such crimes as sexual assault and burglary where the chance of discovering forensic evidence on crime scenes or victims is greatest.

42. The legal infrastructure to support the collection of DNA samples had by then already been established. The CJPOA 1994 included powers to take non-intimate samples from individuals charged, reported, cautioned or convicted for recordable offences from 10 April 1995 onward, or who were convicted of sex, violence or burglary offences before that date if they were still serving a prison sentence at the time the sample was taken.

43. The CJPA 2001 allows the indefinite retention of DNA samples from all criminal suspects, regardless of guilt or innocence, their acquittal or conviction. The Act also permitted police to take samples at the point of arrest, rather than at the point of charge, further expanding the database. Powers were given to the police to keep sample details on their own systems for ease of matching.

44. From the late 1990s a small number of area forces pioneered the practice of taking DNA samples from anyone charged with any recordable offence.

45. The NDNAD comprises a substantial spectrum of personal data. The following fields, derived from a subject access request, comprise a file on the national DNA database:

    (a) Name;

[1] The FSS was the custodian of the NDNAD until December 2005. A Home Office unit is now responsible for regulation of the database.

(b) Date of Birth;
(c) Alias 1;
(d) Alias 2;
(e) Gender;
(f) Country;
(g) Paternity Id;
(h) Ethnic Origin;
(i) Sample Barcode;
(j) Sample Type 3;
(k) Case Class Code: SA;
(l) Case Reference;
(m) Recordable Offences;
(n) Case Reference;
(o) Arrest Summons;
(p) Batch Reference;
(q) Number in Batch;
(r) Gel Number (+Track Number);
(s) Test Type: 3.

46. The existence of a NDNAD profile is flagged on the Police National Computer (PNC), marked against the relevant name and, if relevant, alias entries. The links between the NDNAD and the PNC are detailed further at section B-IV(d) of this witness statement. The domestic courts appeared to be unaware of these links, and three of Lord Steyn's five factors relating to proportionality (summarized in the Court's admissibility decision at p. 4) indicate that he was unaware that, along with the retained bodily material, related information is also retained on the PNC.

47. The NDNAD contains only DNA profiles. A DNA profile is a numerical representation of selected regions of an individual's DNA sequence. Profiles should not be confused with the original samples provided by suspects or volunteers. (The distinction between samples

and profiles is outlined above, at section B-II of this witness statement.)

48. In the current NDNAD system 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. 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 simply not the case. It is incorrect to state that it is 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.

49. The official police reference text *Blackstone's Police Manual: Evidence and Procedure* (Johnson and Hutton, Oxford University Press, 2004, endorsed by the Central Police Training Development Authority) states that, "the purpose behind the taking of [DNA] samples is to enable the process of DNA profiling" (para. 16.6.1, p. 288). This document does not advance any reason for the retention of samples which are of no subsequent forensic value in the system as currently constructed and operated.

50. 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.

51. 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."

52. 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".

53. I am of the view that these broad, generalized purposes simply cannot support the Government's contention that permanent retention of the samples is necessary in a democratic society and proportionate.

54. 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.

55. 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

56. 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 (see section B-II(b) of this witness statement, above) and instead using 13 (as in the US) or 16 (as recommended by Professor Sir Alec Jeffreys) STR loci.

57. 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 DNA samples and include additional loci. Such an argument was outlined recently by the US National Institute of Justice:

> "It can be argued that saving the DNA permits restesting and inclusion of additional loci, particularly newly discovered ones. This would be a lot more efficient that searching out the person, who may not even be living. On the other side, it is argued that the profiles are recorded and that this information is all that is needed, not the DNA itself. Furthermore, those fearful of invasion of privacy are concerned lest the DNA becomes available to unauthorised parties or otherwise be used in ways that would disclose information that ought to remain confidential." (National Commission for the Future of DNA Evidence, National Institute of Justice, US Department of Justice, *Future of Forensic DNA Testing: Predictions of the Research and Development Working Group*, NCJ 183697, November 2000, p. 36.)

It is important to realise that this is purely hypothetical, a speculative assessment of possible future developments in DNA profile generation. It is difficult to see how a speculative, hypothetical argument in favour of retention of the full genetic sequence or 'future diary' of innocent

individuals like the Applicants could ever satisfy the Court's stringent proportionality criteria.

58. Dr. Bramley makes reference to an earlier upgrade at his para. 10.5 (the move from 'SGM' profiling to 'SGM Plus'). He states that:

> "SGM Plus increased the number of markers in the DNA profile from 12 to 20. The consequence was an increase in discriminating power from 1 in 50 million to 1 in 1,000 million. This increased discriminating power can result in either strengthening the case against an individual or eliminating the individual as a suspect. Upgrades of profiles for this purpose would not have been possible in practice without access to original samples."

59. It is important to bear in mind that both of the apparent advantages Dr. Bramley cites (strengthening a case against an individual, or eliminating an individual as a suspect) would both be achieved in any event by the collection and analysis of a fresh sample under PACE powers, which Dr. Bramley accepts in his Witness Statement is standard practice (para. 10.12). Further, the upgrade referred to was a partial upgrade only, with reanalysis of only a tiny percentage of samples undertaken (see the NDNAD Annual Report 2003-04, p. 16).

Miscarriages of Justice

60. 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*. (This is illustrated by Professor Sir Alec Jeffreys' witness statement, and his discussion of the early cases in which DNA analysis was used to disprove involvement of a suspect in a crime; see also the Explanatory Memorandum to Recommendation R (92) 1, paras. 1, 2.) However, this does not justify retention of such information indefinitely.

61. 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.

62. 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.

63. Third, Dr. Bramley gives a wholly exceptional example at his para. 10.7 concerning reanalysis of a sample. Taking the example at its height this is not a sufficient justification, in my view, for permanent retention of such sensitive information for over 4 million individuals within England and Wales. In any event, I note that he does not make clear whether the DNA profile in that case revealed any relevant information, or what alternatives were available to the Criminal Cases Review Commission.

(b) National Automated Fingerprint Identification System

64. 'Fingerprint' is defined by PACE Code D, para. 4.1 and s. 65 PACE as any record, produced by any method, of the skin pattern and other physical characteristics or features of a person's fingers or palms.

65. Fingerprints must be classified in order to make the task of searching a database to find a match among fingerprint form records possible. The standard manual classification system, the 'Henry System,' provided 1,024 primary classifications, with the 16 most common of those 1,024 primary classification categories being further subdivided into

thousands of secondary, tertiary, major and minor sub-classifications. This shows that while there are many variations within fingerprints there are also many similarities.

66. Paul Bogan has summarised the distinctions between the manual 'Henry System' and the current computerised system as follows:

> "The manual system is complex, permitting great power of discrimination. For computer classification purposes, the classification system is simplified and more computer-friendly. Ten-finger fingerprint forms are divided into major classes by pattern type, then sub-divided into a number of sub-classes. Added sub-classifications further divide the collection. The classification system results in many thousands of classification groupings being possible. Scene marks are then searched against the force database.
>
> Initially each police force or small consortia of forces developed their own computerised systems, eventually leading to a nationwide integrated system." (Bogan, *Identification: Investigation, Trial and Scientific Evidence*, p. 270).

67. In 1984 the first automatic fingerprint recognition system was installed at Scotland Yard. Between 1984 and 1998 this expanded to become the National Automated Fingerprint Identification System (NAFIS). 'Tenprint' fingerprint forms are manually loaded onto the database and the fingerprints are classified. Each 'tenprint' record consists of ten fingerprints and two palm prints.

68. If the scene of crime marks are suitable they are scanned onto the computer. A number of key features and possible/ probable pattern-types are indicated to the computer. The computer determines geographical references between the key features indicated. It can then be asked to search the reference database for possible matches to characteristics disclosed on the tenprint forms. The computer searches for similarities, and then produces a 'candidate list' of any possible matches it finds, in order of probability. This does not mean that the match with the highest probability is a positive identification; often this will be found not to be the case when checked manually.

69. Although the Police Information Technology Association (PITO) has responsibility for NAFIS, the service provider is a private company with its headquarters in Los Angeles, US.

70. Fingerprints can now be taken electronically provided that they are taken using such devices as the Secretary of State has approved for the purposes of electronic fingerprinting (s. 61(8A) PACE). 'Livescan' is an approved computerised method of capturing fingerprint images without the use of ink. It uses a device that can immediately transmit for processing on the NAFIS system. Hand-held computer terminals can be used by police at crime scenes or on the roadside to check the identity of individuals against NAFIS and the PNC. If a corresponding fingerprint form is held on file, identity is usually confirmed immediately (live identification). The Livescan system is gradually being introduced throughout England, Wales, Scotland and Northern Ireland.

71. The taking of fingerprints and palm prints is governed by ss. 61 and 63A PACE. Fingerprints and palm prints are now retained permanently by the police, regardless of the guilt or innocence of the individual. Where a person's fingerprints are to be taken without their consent, reasonable force may be used if necessary (Code D, paras. 4.3 and 4.4).

72. Millions of sets of prints are stored on NAFIS although no up-to-date official figures are available for the database's size. In the early 1990s the National Fingerprint Collection consisted of 4.5 million sets of fingerprints, and according to PITO in 2003:

> "Currently, the national databases held on the system consist of more than five million sets of prints… By 2004, the system will be capable of holding 8.2 million sets of prints." (PITO website,

'what we do,' available at http://www.pito.org.uk/what_we_do/identification/nafis.htm.)

In early 2005 a PITO document referred to, 'a combined database in excess of six million records, or 12 per cent of the UK adult population.' (PITO website, 'what we do,' http://www.pito.org.uk/what_we_do/identification/ident1.html;) and in a PITO document dated 6th March 2007 reference is made to "the national fingerprint collection of over 7 million prints" (PITO website, 'Lantern,' http://www.pito.org.uk/products/lantern.php). This is the most recent figure publicly available.

73. The system continues to expand rapidly, with approximately 120,000 new fingerprint sets added each year.

74. As in the case of the NDNAD, official documents often refer to the fingerprint database without distinguishing between those who are on it because they have been convicted of a crime and those individuals, such as the applicants, who remain on the database despite their acquittal or other finalising of the charges against them. PITO, for example, refers to the database as a "national database of tenprints from offenders." (PITO website, 'what we do,' http://www.pito.org.uk/what_we_do/identification/nafis.htm;.)

(c) Police National Computer

75. The Police National Computer (PNC) began as a limited, purpose specific database in 1974, with Stolen Vehicles as its initial database. Since then, additional applications have been implemented almost every year. The PNC now contains a vast array of information and is accessible through more than 10,000 computer terminals nationwide.

76. Four types of individual now have nominal records on the PNC: (a) convicted persons, (b) acquitted persons, (c) those who have received a penalty notice for disorder, and (d) those who were arrested pursuant to

the CJPA 2001, such as the applicants, and whose DNA profiles remain on the NDNAD or whose fingerprints remain on NAFIS. These categories are detailed in the attached document, marked as CG3, Association of Chief Police Officers (ACPO), *Retention Guidelines for Nominal Records on the PNC: A Consultation Document*, 9th February 2005. No distinction is made between these different categories of police record.

77. The PNC is not only accessible to the police, however. A wide range number of non-police groups are entitled to access information held on the computer. In total, 56 bodies currently have access to the PNC. They include governmental intelligence agencies and the secret service, government departments and even groups such as the Association of British Insurers. Until 2003 British Telecom, the national telephone service, had PNC access. The full list of bodies with PNC access (provided by the Police DNA and Fingerprint Retention Project in April 2005) is attached as document CG4.

78. Individuals applying to work in particular jobs are subject to checks by the Criminal Records Bureau (CRB), with police records checked through the PNC. If the individual is applying for a job with children or other vulnerable groups an 'enhanced criminal record check' may be required, and this may reveal non-conviction information retained on the PNC.

79. The PNC is linked to the Schengen Information System, a Europe-wide data system designed to allow what PITO describes as 'criminal information' be shared with participating countries.

80. PITO describes the PNC as holding 'extensive data on criminals, vehicles and property,' but, again, 'criminals' includes innocent, unconvicted individuals such as the applicants (detailed in section B-IV(d) below). The Metropolitan Police refers to all PNC records as

'criminal records,' again disregarding the distinction between different categories of person whose data is retained on the PNC.

(d) Links between NDNAD, NAFIS and the PNC

81. Both the NDNAD and NAFIS are connected to the PNC.

82. Since 1976 the Police National Computer (PNC) has been linked to the National Fingerprint Collection. NAFIS and the PNC are now connected by a Phoenix Number. Individuals whose fingerprints were previously taken by police can be identified, not only be an expert examining their prints, but also by any non-expert from any of the 56 agencies listed in attached document CG4 with access to the PNC. Further, the use of the Livescan system now means that those individuals, such as the applicants, whose fingerprints are retained may also be identified by any police officer using a hand-held computer terminal at the side of the road.

83. As outlined at section B-IV(a) above, the placing of an individual's DNA profile on the NDNAD also necessarily requires a record to be made on the Police National Computer (PNC). The NDNAD and the PNC are linked, and it is the PNC which provides details of the identity of the persons whose profiles have been loaded onto the NDNAD.

84. Statements in the domestic courts concerning the absence of biographical information and the availability of personal information only via a 'hit' on the NDNAD with a crime scene sample are incorrect as they ignore this crucial link between the NDNAD and the PNC.

85. Following the Court of Appeal decision in *S and Marper* the Information Commissioner's Office (ICO) indicated that the court's decision had been largely based on ignorance of this NDNAD/ PNC link.

86. The Information Commissioner's Office is a UK independent statutory authority reporting directly to the UK Parliament. It oversees and enforces compliance with both the Data Protection Act 1998 (DPA) and Freedom of Information Act 2000 (FOI). The DPA applies to 'personal data,' data about identifiable living individuals. Those who decide how and why personal data is processed (data controllers) must comply with certain rules of good information handling, known as the 'data protection principles'. These principles draw on both EU and ECHR approaches to privacy. Those about whom data is processed (data subjects) are also provided with a number of rights which they may use to access certain information about them, as well as control the way in which it is processed in some cases.

87. In the attached letter (provided to the non-governmental organization Liberty on 14th June 2004, marked as CG5) Mr. David Smith, Assistant Commissioner, Information Commissioner's Office, details how the two databases interlink. He explains:

> "DNA profiles are not retained in isolation. To be of any value for policing a profile must be associated with other data. The details that are retained with the profiles on the NDNAD include 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." Phoenix is the criminal records application on the PNC. This number therefore provides a link between the NDNAD and the PNC….
>
> The effect of this system is that if an individual is identified through his/ her DNA profile there is a simple and direct link to that individual's full PNC record." (CG5, pp.1, 2.)

88. PNC records have not been retained for life in the past. In circumstances such as those of the applicants, their PNC record,

associated DNA profile on the NDNAD and any associated information would previously have been deleted within 42 days of their acquittal/ a decision to drop charges against them. Even in cases involving convictions, PNC records would be deleted following fixed periods of time set out in the Rehabilitation of Offenders' Act 1974. These time periods differed according to the nature of the offence, the length of sentence, and other factors.

89. Mr. Smith explains at p. 2 of his letter that this position was changed by the CJPA 2001:

> "This Act removed the requirement on the police to destroy DNA profiles of those who are not prosecuted or who are acquitted… [Those] DNA profiles are of little or no value to police if they are retained in isolation. The question therefore arose as to what information could be retained alongside a DNA profile. This is information that is part of the PNC record and would otherwise have been deleted shortly after the decision not to prosecute or to acquit the individual.
>
> The police, perhaps not surprisingly, were keen to retain the full PNC record associated with any DNA sample. This would effectively bring an end to the removal of any PNC record once it had been created during the lifetime of the individual the record related to. This would be the case even for an individual who had been able to establish his/ her innocence of any offence." (CG5, p. 2.)

90. It, of course, stands to reason that some demographic/ biographical data must be retained if the DNA profile is to be retained, as without an identifier the profile is useless. In the ACPO document, *Retention Guidelines for Nominal Records on the Police National Computer: A Consultation Paper* (February 2005, attached as CG3), this is accepted:

> "PACE, as amended by The Criminal Justice and Police Act 2001, removed the requirement for the Police to destroy DNA and fingerprint samples, relating to persons following acquittal at court or a decision not to prosecute. The Act, by definition, requires the details of non-convicted individuals to be retained. Using the PNC to record associated demographic information enables a link to be made to DNA and Fingerprints."

91. The ACPO document goes on to state that, "in order to link these samples to an individual, the police need to keep a demographic record on PNC." The attached letter from the Information Commissioner's Office contains a rebuttal of this point, as – while some form of identifier is needed to identify the profiles – they recommended an alternative system of identification, rather than retaining the full PNC 'criminal record.' Mr. Smith details the Information Commissioner's Office view that,

> "the purpose of the changes introduced by the 2001 Act was to enable the retention of the information necessary to identify someone from a DNA sample rather than to bring about the lifetime retention of the complete criminal record." (CG5, p. 2.)

The Information Commissioner's Office discussed this issue with ACPO and recommended that, if any information were to be retained on the PNC, it should only be information required to assist identification. This might include details such as height or eye colour, but not details related to the alleged offence, for example. In addition, the Commissioner's Office recommended that a record which would otherwise fall to be removed from the PNC should not only be stripped down to the bare identifiers, but should 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" (pp. 2 - 3). This, and other minimum

safeguards recommended by the Commissioner, were not implemented.

92. The ACPO document does not consider the Commissioner's argument that, if the profiles are to be retained at all, an alternative database or subset of the database for identification purposes only is required rather than the PNC. ACPO instead states that,

> "The obvious place for this data, referred to as 'Identifiers', to be held is the PNC. Where the individual concerned has no previous offending history, their data will be held alongside that of persons with previous convictions. This represents a sea change for the police and other users of the PNC.
>
> Where the only reference on a PNC record is that relating to an Acquittal, or CJ Arrestee [unconvicted individual such as either of the applicants], all users of PNC should be aware that the subject is **free from any taint of criminality.**
>
> Access to historic acquittal and arrest event details on a national database represents a substantial change for the police service. Police officers and police staff will need to make professional judgements based on the nature and age of the record.
>
> Providing the police service has robust and consistent business processes in place to ensure that access is not abused, t**he truly innocent need not fear the existence of such records** (emphasis added)."

93. There is an obvious mismatch between the aspiration that all PNC users should be aware that the individual is "free from any taint of criminality" and the reference to the "truly innocent". The implication is that many of those whose records are retained are technically

innocent, but not truly innocent. This division of the unconvicted population into the truly innocent and the guilty, with S and Mr. Marper somewhere in between, is of particular concern in a common law jurisdiction with a tradition of the presumption of innocence.

94. The PNC records of unconvicted individuals such as S and Mr. Marper are not only accessible to the police. An enormously wide range of other public and private bodies have PNC access (as detailed at section B-IV(c) of this witness statement and in attached document CG4). The impact of retention of this information is not only a theoretical one, relating to presumptive innocence and presumptive privacy under Art. 8 ECHR, but also a practical one.

95. For example, PNC information such as this may be available to employers (through the Criminal Records Bureau) if the individual requires an 'enhanced criminal record check' for a job working in a hospital or school. The practical import of S and Mr Marper's remaining presence on these databases is that, if they apply for a job which requires an enhanced criminal record check their prospective employer is likely to be informed of their police record.

96. Further, other third parties may demand access to PNC records using the practice of 'enforced subject access' described by Mr. Smith at p. 3 of document CG 5. This is the means whereby a third party, usually a prospective employer, requires an individual to use his right of access to police records for the third party's benefit. In this case, any employer could demand access to S and Mr Marper's records, not only an employer such as a hospital or school. Many employers make a subject access request to the police, and showing the response to the employer, a condition of employment. Such 'enforced subject access' will include the full PNC record. Mr. Smith condemns this practice and the practical implementation of the CJPA 2001 at p. 3:

> "It remains a substantial but lawful intrusion into individuals' privacy. Even if reduced in scope it will remain so. We should be particularly concerned if the consequence of retention of DNA profiles on the NDNAD in acquittals and discontinued cases is that these records are also available on the PNC and therefore become available through enforced subject access to employers and others for the lifetime of the individual concerned."

(e) Police Elimination Database

97. In addition to the databases that combine previous suspects and convicted criminals' information, NDNAD and NAFIS, England and Wales also has a separate forensic database, the Police Elimination Database (PEDb). The purpose of this database is to eliminate police officers from inquiries, as their genetic material and fingerprints may sometimes contaminate a crime scene and become intermingled with the offender's and/ or the victim's prints and genetic material.

98. However, the database operates on the basis of an inbuilt structural presumption that police do not commit crimes, and this compounds the stigma associated with an individual's presence on the NDNAD and NAFIS reference database and underlines Liberty's concern regarding those databases' undermining of the principle of presumptive innocence.

99. The PEDb does form part of NAFIS, but it is a separate database within that system. It is retained and accessible locally only, not nationally. It is not subject to speculative searches when NAFIS is being searched against a scene of crime sample or prints from a suspect. It is not linked to the PNC.

100. Home Office Circular 23/2005 was implemented on the 25th April 2005 and remains in force (attached as document CG6). The

Circular provides guidance to police forces on fingerprints and the use of the PEDb.

101. The Circular outlines the impact of Regulation 18 of the Police Regulations 2003. It provides that every member of a police force shall in accordance with the directions of the Chief Officer have his fingerprints taken. The fingerprints shall be kept separately from fingerprints taken in other circumstances (i.e. from suspects and convicted criminals) and shall be destroyed on leaving the police force except where, by reason of a statutory transfer, the officer becomes a member of another force, in which case the records and copies should be transferred to the chief officer of the new force. On transfer to a force other than on a statutory transfer, a new set of fingerprints should be taken.

102. Fingerprints are taken for elimination purposes only and will be held in an electronic format in a discrete database (on the local PEDb) within NAFIS under the authority of the relevant Chief Officer. The PEDb may only be interrogated by the Force Fingerprint Bureau of the officer concerned.

103. Where fingerprints are found at the scene of a crime, a search of the PEDb will be made automatically to identify and eliminate from enquiries the fingerprints of officers and others attending crime scenes whose fingerprints are held on the PEDb. The search of the PEDb is for elimination purposes only and will be conducted prior to search through "the main criminal and intelligence fingerprint database". The Circular states that,

> "the purpose of obtaining fingerprints is to allow for checking for innocent marks left unwittingly at scenes-of-crime against fingerprints obtained in the process of crime investigation."

It also admits that,

> "it is to be noted that because of the difficulties in identifying all attendees at scenes-of-crime and in order to streamline the process, the marks are searched against the entire (individual force) PEDb and not against the profiles of individual officers."

This amounts to a structural assumption in the database's operation that police officer prints found at the scene of a crime are there through accidental contamination, not criminal activity.

104. This presumption is rebuttable, and it is possible to search the PEDb for purposes other than elimination purposes, but only in what the Circular describes as "very exceptional circumstances". In such rare cases, the authority in writing of a chief officer will be required.

105. The safeguards associated with the PEDb also differ markedly from those concerning the NDNAD. The responsibility for management and security of the PEDb rests with the force fingerprint bureau on behalf of the Chief Officer. Each officer, support staff or worker is identified by a unique reference number - the 'Police Worker Reference Number'. The composition of this number includes the force code, type of record (officer/special/support), and unique identifier. This enables NAFIS to place the record in the correct part of the local database and restricts access to the record to fingerprint staff from that force only.

106. The Home Office has drafted a standard letter which should be issued to new recruits and serving police officers, as appropriate, explaining why fingerprints are being taken and the circumstances in which they will be used. Officers serving prior to the coming into force of this rule are not required to provide their fingerprints.

(f) Future Developments

107. According to the government's Science and Technology Strategy, work is currently being undertaken to find methods of producing "lab on a chip" technology that would permit roadside analysis of DNA samples linked directly to the NDNAD.

108. Research is also being conducted on the development of a hand-held DNA testing kit to be carried and operated by police officers during regular patrols (not when attending a crime scene). The device would be connected to the national NDNAD via the Airwave system.

109. With such a development, the effect of an individual remaining on the NDNAD and the PNC for life following an acquittal or charges being dropped against him/ her is that at routine roadside patrols, if asked to provide a sample a 'match' will register on the police officer's hand-held device.

110. This would be the DNA equivalent of the Livescan system which already links to NAFIS and is currently being expanded across the country.

111. In addition to the NAFIS system, since April 2005 rollout of a new system has started, IDENT1. This is the "next generation of identification services for the police service." It will allow routine identification using finger and palm prints across Scotland and England and Wales.

112. Automated 'risk-based' and 'intelligence-based' searches of the PNC are also expanding, for example through Automatic Number Plate Recognition (ANPR) of cars in a particular area. Those cars which register a 'hit' on the PNC are then stopped, the driver questioned and, in many cases, the car searched. If Airwave and Livescan follow this pattern the lifetime impact of remaining on the NDNAD, NAFIS and/ or the PNC is clear.

C. CONCERNS RELATING TO RETENTION UNDER THE CURRENT SYSTEM

I.

Criminal Records Bureau

113. The Criminal Records Bureau (CRB) was introduced in 2002. It provides a disclosure service to enable organisations to gain access to "important criminal and other information" (ACPO Consultation Document) for recruitment and licensing purposes. Individuals who have been acquitted or had charges against them dropped, yet remain on the NDNAD and PNC, may discover that this information is disclosed to potential employers and that their job applications are therefore unsuccessful. Complaints have been made concerning such disclosure to the Information Commissioner, who has seen fit to issue Enforcement Notices against three police forces requiring them to remove specified data from the PNC or local force systems.

114. ACPO recognises that current access by non-police users to PNC records is problematic when dealing with innocent individuals who have never been acquitted of a crime. They suggest that access to such records should be restricted to police users only, but there is no implementation period for this suggestion. Besides, they suggest that where the individual is the subject of an enhanced check under the CRB vetting process, this information should continue to be disclosed. The only new safeguard proposed is that, "in those cases the data should be dealt with as intelligence and only disclosed on the authority of the Chief Officer or delegated authority".

II. Disclosure to Others and the Inadequacy of Existing Safeguards

115. In addition to the Information Commissioner's concerns regarding inadequate safeguards to prevent inappropriate disclosure, in a number

of individual cases highly personal information has been revealed due to those inadequate safeguards. For example, 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.[2]

III. Racial Profiling

(a) Disproportionate Representation of Black and Minority Ethnic (BME) Males

116. The NDNAD has also been criticised by various groups on the basis that it contains an extreme over-representation of Asian and black individuals, and there is growing concern about this leading to racial profiling in criminal investigations. Black men are four times more likely than white men to be on the NDNAD, with 32% of black men (from the general population) profiled on the database compared to 8% of white men.

117. In itself, regardless of its disproportionality when compared to the white male population or conviction rates, the 32% figure is highly problematic. One black male in three in England and Wales is presently - and, therefore, permanently - on the NDNAD. This remarkable figure was provided by the Commission for Racial Equality, Independent Race and Refugee News Network (see attached article CG9) and the *New Scientist* (see attached article CG10). .

118. This racial bias within the NDNAD is of particular concern given the language used in official reports, referring to the 'active criminal population,' the 'criminal database' and the 'offenders' register'. Home Office documents, government Ministers and even the police themselves refer to the NDNAD in these terms, making no distinction between those present on the database because they have voluntarily submitted a sample during an investigation, they were

[2] 'Witness told in court he has HIV,' *The Guardian*, 25th May 2004; 'Inquiry into HIV court blunder,' *BBC News*, 25th May 2004.

arrested on suspicion of a crime for which they were later acquitted or the prosecution did not proceed, those who are convicted of minor offences, those who are convicted of serious offences, those who received no prison sentence, those who have completed their sentence and those who are serving life imprisonment. The official and quasi-official use of such inaccurate, generalised, discriminatory language is problematic in itself, for those of any racial or ethnic background who are profiled on the NDNAD. However, given that 1 in 3 black males is on the database the impact of such language is arguably heightened when considering its impact on that particular racial group.

IV. Research Projects

119. A further concern relating to possible abuse and misuse of retained genetic information is the authorisation by the State of research projects using this information. This concern relates, in particular, to research on DNA profiles stored on the NDNAD. (The United Kingdom Government denies that any research is or has been carried out on samples obtained under PACE for the purposes of the NDNAD.)

120. Since 1995 the Home Office and the previous NDNAD custodian, the FSS,[3] have authorised a number of research projects, including one study on extracting statistical information on ethnicity from STR profiles.

121. Most of the research to date has been done by the FSS itself, but given the inadequate safeguards in place there are no guarantees that it will be limited as such in the future.

122. This is not a UK-specific concern. Possible future misuse is one of the reasons given by many countries for immediate destruction of DNA samples after the DNA profile has been created, even when

[3] The FSS was the custodian of the NDNAD until December 2005. A Home Office unit is now responsible for its regulation.

the criminal offence in question is still being investigated (New Zealand, Germany, Sweden, Denmark and the Netherlands; see further G. Gardiner, *DNA Profiling: Information Paper No. 22/01*, 2002, Victorian Parliamentary Library, Australia, p.16). In 1992, the National Academy of Sciences in the US recommended that DNA samples be destroyed "promptly" after analysis, as:

> "In principle, retention of DNA samples creates an opportunity for misuses - i.e., for later testing to determine personal information. In general, the committee discourages the retention of DNA samples…. Investigation of DNA samples or stored information for the purpose of obtaining medical information or discerning other traits should be prohibited, and violations should be punishable by law." (Committee on DNA Technology in Forensic Science, National Academy of Science, *DNA Technology in Forensic Science*, National Academy Press, 1992, pp. 116, 122).

123. The National Institute of Justice also predicted wider future research using DNA profile data on the US equivalent of the NDNAD (considered below at section D-IV of this witness statement):

> "As [the database] enlarges and if it is broadened to include persons convicted of a larger variety of crimes, it might be possible that statistical studies of the databases could reveal useful information. Inventive researchers may glean useful information of the statistical sort. At the same time, there would need to be protection against misuse or use by unauthorised persons." (National Commission for the Future of DNA Evidence, National Institute of Justice, US Department of Justice, *Future of Forensic DNA Testing: Predictions of the Research and Development Working Group*, NCJ 183697, November 2000, p. 36.)

124. This type of research appears to be precisely what is envisaged by the broadened, sweeping justifications for future use of data set out in PACE as amended.

V. Familial Searching

125. A new procedure is being used by the FSS which has never been subject to parliamentary scrutiny. In cases where a DNA sample obtained from a crime scene has not matched an existing profile on the NDNAD, this process is used to identify those on the database who have partial, 'familial matches' which suggest that a relative may be implicated. The relatives of the familial match are invited to volunteer to give samples for further investigation.

126. Familial searching is a Pandora's box in relation to false paternity. Information derived from subsequently obtained DNA samples may reveal that an individual's presumed father is not, in fact, biologically related, and no safeguards or even basic guidance exist to prevent disclosure of such intimate information.

127. Further, an approach to a relative of an individual based on a partial familial match necessarily involves revealing that the individual in question is on the NDNAD himself or herself. Revealing this information to relatives without consent is highly problematic.

D. FORENSIC DATABASES: COMPARATIVE SUMMARY

I. Overview

128. The National DNA Database (NDNAD) of England and Wales is the largest in the world. This is the case not only in relative terms (adjusted according to population size), but it is also the largest in

absolute terms. This clear fact is accepted by the Home Office, which states on its website that:

> "The UK's database is the largest of any country: 5.2% of the UK population is on the database compared with 0.5% in the USA. The database has expanded significantly over the last five years. By the end of 2005 over 3.4 million DNA profiles were held on the database – the profiles of the majority of the known active offender population."[4]

129. By December 2005 the NDNAD contained the DNA profiles of over 3.6 million people (NDNAD Annual Report 2004-05, p. 6). The Annual Report for 2004-05 is the last publicly available annual report.

130. 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.

131. Internationally, the NDNAD's closest competitor in absolute size terms is the Combined DNA Index Systems Database ("CODIS") the national DNA database of the US, which in January 2007 stood at 4,274,700 profiles, comprised of 163,689 forensic profiles and 4,111,011 Convicted Offender profiles (http://www.fbi.gov/hq/lab/codis/clickmap.htm

132. The NDNAD is unique internationally in retaining samples and 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.

[4] Home Office website, http://www.homeoffice.gov.uk/science-research/using-science/dna-database/ (reference correct as of the 13th March 2007).

133. The term 'national' DNA databases is used throughout these comparative summaries. The term 'national' in this context does not imply universality or scale; it is meant simply to distinguish databases that operate across a country from an individual state or regional database, such as those operated in the various internal states or federations of certain territories, e.g. Australia. It does not connote a comprehensive, universal database.

134. The purpose of submitting this comparative material to the Court is to demonstrate the spectrum of approaches adopted by other democratic societies, and to illustrate where on that spectrum the UK's position lies. Recent case law of the Court has confirmed that such material is relevant in assessing both whether there has been an interference with a Convention right and whether such interference is justified (*Goodwin v UK,* App. No. 28957/95, [2002] All ER (D) 158; *Hirst v UK,* App No 74025/01, [2004] All ER (D) 588). It is also noted that that the Court has asked the parties to supply information relating to the comparative position in its letter dated 19th January 2007.

135. The comparative material clearly demonstrates that the UK's approach to the issues raised by the present case is grossly out of kilter with that adopted elsewhere, both those countries within the remit of the Convention and other democratic common law states with similar constitutional traditions to the UK.

136. In relation to genetic databases, even within the UK itself England and Wales goes far further than Scotland or Northern Ireland. Research suggests that there is no discernible benefit in terms of 'clear-up' or 'conviction' rates when the crime statistics of England and Wales are compared to those of Scotland (see the Witness Statement of Robin Williams for details of this research).

II. DNA Databases in European Union and Council of Europe Countries

(a) Research Methodology

137. This outline of the approach adopted in European countries is in part based on a research study carried out by Liberty in January – May 2005. .

138. Standard academic methodology was followed for the collation of this information. Much of the comparative common law information in particular is supported by research and findings of the Irish Law Reform Commission, the Human Genetics Commission and the Report of the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council, *Essentially Yours: The Protection of Human Genetic Information in Australia*.

139. Further, I am aware of additional details relating to the policies adopted in a number of Council of Europe Member States and internationally as the result of consultancy work undertaken for government departments, the Council of Europe and certain non-governmental organizations (NGOs).

140. In relation to the materials based upon information gathered by Liberty in 2005, their methodology was as follows. Approaches were made to each Embassy from the Member States of the Council of Europe seeking information relating to national DNA database practices. In certain cases Embassies referred Liberty to other sources.

141. The key (but not sole) issues identified in Liberty's correspondence with each Embassy included:

(a) Whether a national DNA database is in operation;

(b) What information is stored on any database (DNA profiles or samples);

(c) Which individuals are listed on the database (all individuals convicted/ charged/arrested in connection with a criminal offence);

(d) How long the genetic material is stored for;

(e) Who can access the information and why;

(f) What privacy safeguards exist.

(b) Findings

142. Of the 42 countries researched in Liberty's comparative study, the NDNAD of England and Wales is the most extensive both in terms of its size and the freedom to obtain, use and store genetic information enjoyed by its government. In terms of size the NDNAD dwarfs its nearest rival. The summary of findings is attached in table form, marked as CG3.

143. Of the countries surveyed, DNA samples and profiles 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).

144. Since Liberty conducted its study the Serious Organised Crime and Policing Act 2005 came into force. Under that Act all offences in the UK are arrestable, so that individuals suspected of committing the most minor crimes may be required to provide a sample for DNA analysis against their will. This development has moved the UK even further from the approaches adopted by the other countries researched for Liberty's study.

145. 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).

146. 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.

147. A recent case in Germany (*Mooshammer*) illustrated that abuses can occur even in jurisdictions where it is claimed that individuals will be removed from the national database following acquittal and in which strong privacy safeguards are present.

(c) German Constitutional Court Judgments

148. The German national DNA database is the second-largest in Europe, standing at 380,000 profiles compared to the NDNAD of England and Wales' estimated 3 million. The differential is huge, with the NDNAD exceeding the German database by 800%, and if weighted according to population the differential would be even larger (Germany's population exceeding 82 million, with the population of England and Wales at 52 million). Nevertheless, as the closest comparison to the NDNAD within Europe, and a country which has recently examined the constitutionality of provisions concerning the retention of DNA material, it merits close review.

149. In Germany a National DNA Database was established in 1998 by the legal provisions of the DNA-Identitätsfeststellungsgesetz (DNA-Identification Act 1998, 07.09.1998). The DNA database is

operated by the Federal Bureau of Criminal Investigation (Bundeskriminalamt). The database contains DNA profiles which are gained in compliance with Sec. 81e-g German Criminal Procedure Code (StPO) and Sec. 2 DNA-Identification Act. The relevant legislation is attached as document CG16.

150. The blood samples or other body cells taken from the accused shall be destroyed without delay as soon as they are no longer required for the purposes of the criminal proceedings for which they are taken or in other criminal proceedings pending, cp. Sec. 81 a Abs. 3 StPO. Once the profiles are generated the samples' purpose is spent and they are destroyed.

151. The German DNA Database may only contain – temporarily - DNA profiles from accused people:

(a) that have very likely committed a crime ("hinreichender Verdacht"), or,

(b) for the purposes of establishing identity in future if the nature of the offence or its means of commission, the accused's personality or other information provide grounds for assuming that new criminal proceedings shall have to be conducted against the accused person for criminal offences of substantial significance particularly,

- a serious or less serious criminal offense against sexual self-determination (Sec. 174- 184f German Penal Code), or
- serious bodily injury, theft in a particularly serious case or blackmail.

152. DNA profiles may also be stored in the national DNA Database from people that are convicted of a crime, or who are not convicted only by reason of their incapacity or mental disease if their crime has not yet been deleted from the Federal Central Criminal Register.

153. DNA profiles from other people such as witnesses must not be stored in the German database.

154. The storage, alteration and the use of DNA profiles from the DNA Database is forbidden if the related person has been found not guilty (Sec. 8 Abs. 3 BKAG). In that case, DNA profiles must be deleted from the DNA Database. (Under specific, limited circumstances they may still be kept for use in later proceedings.)

155. In the case of profiles remaining on the database due to the conviction of the individual, there are no legal provisions determining a deadline after which DNA profiles must be deleted from the DNA-database. However, at regular intervals the Federal Bureau of Criminal Investigation has to check whether DNA profiles are still relevant or can be deleted form the database. Those periods must not exceed 10 years if the person is an adult and 5 years if the person is an adolescent, Sec. 32 Abs. 3 BKAG.

156. Access to the DNA database can only be granted in connection with criminal proceedings, averting danger ("Gefahrenabwehr") and for international legal assistance, Sec. 3 S. 3 DNA-Identification Act.

157. Only staff from the Bundeskriminalamt and the Federal State Bureaus of Criminal Investigation ("Landeskriminalämter") may receive DNA profiles from the database. Ordinary police forces as well as the Federal Border Guard ("Bundesgrenzschutz") etc. have no access to the DNA database.

158. DNA-examinations pursuant to Sec. 81f StPO may be ordered only by a judge. The affected person may appeal against that order.

159. The German DNA database system has been subjected to scrutiny by the German Constitutional Court. There are two relevant

cases, file number BVerfG, 2 BvR 1741/99 (2000) and file number BVerfG, 2 BvR 1841/00 (2001).

File No. BVerfG, 2 BvR 1741/99 (2000)

160. On 14 December 2000 the Constitutional Court held that the retention of DNA material did fall within the right to privacy under the *Grundgesetz* and Art. 8 ECHR. The Court emphasised that the retention of DNA constituted an inherent and substantial infringement upon private life which had to satisfy a stiff standard of justification.

161. In light of this finding, the Court considered the constitutionality of the statutory provisions governing DNA retention. The Court held that the provisions governing DNA retention in the Law of Criminal Procedure 81G STPO were constitutional, but they passed constitutional muster only because:

> (a) only the DNA of suspects associated with "substantial" crimes (murder, armed robbery, sexual assaults) was retained, and
>
> (b) the DNA material in question was subject to the same data control laws that regulate access to information on criminal records, which require that all records pertaining to convicted criminals be removed after a statutory time period, and that the records relating to suspects are removed on acquittal.

162. The legislation satisfied the proportionality test only because both these requirements were in place.

163. The Court also indicated that the retention of "extra" DNA material (samples rather than merely profiles) which was more than what was strictly necessary for identification purposes would violate the core right to human dignity and was therefore inherently unjustifiable.

File No. BVerfG, 2 BvR 1841/00 (2001)

164. In a second decision, given March, 15th, 2001 the Constitutional Court applied its approach in the first case, and emphasised that lower courts had to be prepared to apply a stiff proportionality test in determining whether to permit the use of retained DNA material under the legislation: one decision was reversed and referred back to the lower court on the basis that the offence in question was not substantial enough to warrant the retention of the DNA material.

(d) The Netherlands

165. 152. The provisions of Dutch law relating to the retention of DNA samples and profiles was considered recently in an admissibility decision by the European Court of Human Rights in *Van der Velden v The Netherlands,* Application no. 29514/05, 7 December 2006, which concerned the compatibility of the Dutch DNA Testing (Convicted Persons) Act ("Wet DNA-onderzoek bij veroordeelden") with Article 8.

166. The Court found that the retention of DNA samples was an interference within Article 8:

> "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).

167. This interference was justified within the exceptions in Article 8(2) on the basis that the provisions of the Act limited to "persons who have been convicted of offences of a certain seriousness".

> "The Court further has no difficulty in accepting that the compilation and retention of a DNA profile served the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others. This is not altered by the fact that DNA played on role in the investigation and trial of the offences committed by the applicant. The Court does not consider it unreasonable for the obligation to undergo DNA testing to be imposed on all persons who have been convicted of offences of a certain seriousness."

168. The key distinguishing factors are therefore the following safeguards and limitations set down in the Dutch Act:

(a) A sample can only be ordered to be taken from person who has been convicted of an offence carrying statutory maximum prison sentence of at least four years: s. 2(1).

(b) 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

(c) Examples where DNA investigations can play no meaningful role, or where the convicted person is also unlikely be able to commit an offence in future (such as a case of battered wife syndrome): s. 2(1)(b).

(d) DNA profiles can only to be processed for the purpose of the prevention, detection and prosecution and trial of criminal offences: s. 2(5).

(e) The duration of retention of the DNA samples and profiles are strictly laid down by Decree: the sample is retained for 30 years if the offence carries a statutory sentence of 6 years or more, and for 20 years where the sentence is up to 6 years - DNA (Criminal Cases) Tests Decree (Besluit DNA-ondersoek in strafzaken).

(f) 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: s. 6(3).

(d) Other Relevant European Information

169. Other DNA projects have been developed in Europe alongside criminal databases. Programmes such as "The Book of Icelanders" have seen the development of a national health database and the Genoma Espana initiative and UK's Biobank, although they are more limited databases, were similarly established to provide services to the scientific and healthcare communities.

170. The Icelandic developments merit examination. In 1998 the Icelandic Parliament passed the Act on a Health Sector Database which authorized a centralized database of non-personally identifiable health data for use in producing "new or improved methods of achieving better health, prediction, diagnosis and treatment of disease". This allows genetic samples to be linked to accurate medical records and genelogical information for recording encrypted medical records of all Icelandic citizens who do not opt out and the linking of this information to databases containing genealogical and genetic information.

171. Although the purpose of the Icelandic database is to facilitate health and medical research, a recent case challenging the provisions of the Act raised a general point of law as to whether the privacy interest in genetic information stored on a national database only applies to the individual concerned, or may also apply to their family and the wider community.

172. In *Guðmundsdóttir v Iceland,* No. 139/1998 (November 27th 2003) the Icelandic Supreme Court held that the daughter of a deceased man had the right to challenge the inclusion of his medical information in Iceland's health database under the principle of privacy in Icelandic law. The case arguably established a general principle that someone other than the source of genetic

information – the "proband" has a legally cognizable privacy interest in the proband's information.[5]

173. Various Council of Europe materials deal with the issue of forensic databases, and I do not detail them here. However, it is important to note that as early as 1992 the Council of Europe Committee of Ministers considered the issues surrounding collection, retention and use of DNA and fingerprint materials. The Committee recommended that:

> "Samples or other body tissues taken from individuals for DNA analysis should not be kept after 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."

III. Fingerprint Databases in European Union and Council of Europe Countries

174. Unlike DNA databases, fingerprint databases are commonplace in European jurisdictions.

175. 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. Details are provided in CG3.

IV. DNA Databases in Common Law Countries

[5] *Icelandic Supreme Court Holds That Inclusion of an Individual's Genetic Information in a National Database Infringes On the Privacy Interests of His Child, 118 Harv. L. Rev. 810 2004 – 2005, at p.812*

(a) Introduction

176. DNA databases for criminal investigation and forensic purposes do exist in all the common law countries surveyed with the exception of Ireland[6] and Cyprus.

177. However, mirroring the European findings, the NDNAD of England and Wales is by far the most extensive database amongst the common law countries, both in terms of its size and the freedom to obtain, use and store genetic information enjoyed by its government.

(b) Canada

178. Canada has a national DNA database, known as the National DNA Data Bank (NDDB). This was created following the DNA Identification Act 1998 ('the 1998 Act').[7] S. 3 of the 1998 Act states that:

> "The purpose of this Act is to establish a national DNA data bank to help law enforcement agencies identify persons alleged to have committed designated offences, including those committed before the coming into force of this Act."

179. The 1998 Act and the Canadian Criminal Code make separate provisions for the search and seizure of DNA material in respect of suspects for investigative purposes to those in respect of convicted offenders.

180. The NDDB consists of two data bank indices: the Crime Scene Index (for profiles generated from samples obtained at scenes of crime) and the

[6] Ireland is currently considering introducing a DNA database.

[7] The 1998 Act was introduced following extensive consultation in 1996 and 1997, which involved police, victim groups, privacy officials, genetic organisations and legal associations.

Convicted Offender Index. No unconvicted individuals are added to the database; it only covers convicted offenders. Further, it does not cover all convicted offenders, but only those convicted of a designated offence (e.g. homicide, serious assault, assault with a weapon). The designated offences are all either serious/ violent crimes or have a high recidivism rate.

181. As of January 2007, the data bank had received 114,840 samples from convicted offenders, and from those entered 108,191 profiles entered onto the Convicted Offender Index; a further 33,189 profiles entered into the Crime Scene Index.

182. Section 4 of the Canadian *DNA Identification Act* emphasises the need to respect the privacy of individuals and place safeguards on the use and communication of both samples and profiles:

> **4.** It is recognized and declared that
> (*a*) the protection of society and the administration of justice are well served by the early detection, arrest and conviction of offenders, which can be facilitated by the use of DNA profiles;
>
> (*b*) the DNA profiles, as well as samples of bodily substances from which the profiles are derived, may be used only for law enforcement purposes in accordance with this Act, and not for any unauthorized purpose; and
>
> (*c*) to protect the privacy of individuals with respect to personal information about themselves, safeguards must be placed on
>
> > (i) the use and communication of, and access to, DNA profiles and other information contained in the national DNA data bank, and
> > (ii) the use of, and access to, bodily substances that are transmitted to the Commissioner for the purposes of this Act.

183. Underpinned by s. 4 of the 1998 Act, privacy-enhancing technologies are used to maintain the confidentiality of data on the NDDB. Both crime

scene samples and convicted offender profiles are only identified by a unique number, and information can only be accessed in the event of a future match. The donor identity of the convicted offender is removed from the genetic information at the time the sample arrives at the data bank. A bar code number links the personal information to the DNA material. The link is protected information that is not accessible to data bank staff, and it is kept by the Royal Canadian Mounted Police's Canadian Criminal Records Service. The system is akin to that unsuccessfully proposed in England and Wales by the Information Commissioner's Office (see CG5, p.3); in other words, the Canadian system has stronger protection for convicted offenders' profiles than the NDNAD has for unconvicted individuals such as the applicants.

184. DNA profiles are only accessible for defined law enforcement purposes.

185. The Royal Canadian Mounted Police operates the national database. It is subject to oversight from an advisory committee consisting of experts in policing, privacy, bioethics, genetics, medical ethics and law. The committee's task is to balance privacy, legal, ethical and human rights concerns with the latest scientific developments. The committee in its report of 2002 was highly complimentary in relation to the operation of the NDDB and it "applauds the safeguards established to protect the privacy and security of convicted offenders' DNA." (Annual Report of the National DNA Bank Advisory Committee, 2002, available at http://www.rcmp-grc.gc.ca/dna_ac/index_e.htm.)

186. The advisory committee includes the Privacy Commissioner of Canada, the equivalent of the Information Commissioner's Office in the UK.

Canadian DNA Database: Provisions relating to Suspects

187. Section 487.05 of the Criminal Code states that a sample can be seized from a person suspected of having committed an offence. This is restricted as follows:

a. Prior judicial authorisation is required;
b. The judge must have reasonable grounds to believe offence committed, DNA evidence exists, and that the suspect was a person party to that offence (s 487.05(1));
c. The offence must be a designated offence (as defined in section 487.04 – 'designated offences' are offences of a serious and / or violent nature);
d. 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 (s 487.05(2)(a));
e. The use of the samples is restricted to "forensic analysis" which is defined in the *Code* as comparison of DNA from sample with results of DNA from crime scene sample (s 487.08(1));
f. **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(s 487.09).

188. The constitutionality of the provisions relating to suspects was the subject of an appeal before the Canadian Supreme Court in 2006 in the case of *R v S.A.B* [2003] 2 S.C.R. 678, 2003 SCC 60, in which it was held that the provisions of sections 487.04 to 09 were not unconstitutional or a violation of section 8 of the Canadian Charter of Rights and Freedoms (which states "everyone has the right to be secure against unreasonable search or seizure").

189. While it was held that "there is undoubtedly the highest level of personal and private information contained in an individual's DNA" (per Arbour J, at para 48), the provisions relating to suspects were deemed reasonable, and therefore not a breach of sections 7 (which sets out the principle against self-incrimination) or 8 of the *Charter*.

190. This opinion was fundamentally based on the safeguards in the legislative safeguards governing use and communication of DNA samples and profiles, described above and further set out by Arbour J as follows: (per Arbour J at para 4):

> "The process of obtaining a DNA warrant is commenced under s. 487.05 by a sworn information presented *ex parte* to a provincial court judge, who can only grant the warrant if there are reasonable grounds to believe:
>
> (a) that a designated offence has been committed (importantly, the offences for
> which one can obtain a DNA warrant are limited to predominantly serious violent and sexual offences listed in s. 487.04);
>
> (b) that a bodily substance has been found at the place where the offence was committed, on or within the body of the victim, on anything worn or carried by the victim or on or within the body of any person or thing or at any place associated with the commission of the offence;
>
> (c) that the person targeted by the warrant was a party to the offence; and
>
> (d) that forensic DNA analysis of a bodily substance from that person will provide evidence about whether the bodily substance referred to in (b) was
>
> Additionally, the judge must be satisfied that it is in the best interests of the administration of justice to issue the warrant (s. 487.05(1))."

191. As stated above, s 487.09 also provides strict limits on the extent to which samples and profiles can be retained in the absence of a conviction.

Provisions relating to convicted offenders

192. Sections 487.051 to 487.055 apply to the seizure of samples of persons convicted of offences. The following restrictions apply:

a. Judicial authorisation is required;

b. The provisions only apply to three specific categories of offenders:
   (a) Persons convicted of a designated offence after DNAIA 1998 in force (s 487.051);
   (b) Persons convicted of designated offence prior to DNAIA 1998, but whose case is still before the court (s 487.052);
   (c) Persons convicted and sentenced prior to the proclamation of DNAIA, where:
      (1) They have already been declared a "dangerous offender";
      (2) They have been convicted of murder, or
      (3) They have been convicted of more than one sexual offence and serving sentence of imprisonment of at least two years.

193. The constitutionality of the provisions relating to convicted offenders was the subject of an appeal before the Canadian Supreme Court in 2006 in the case of *R v. Rodgers* [2006] 1 S.C.R. 554, 2006 SCC 15, in which a majority held that the provisions of sections 487.051 to 055 were not unconstitutional or a violation of section 8 of the Canadian Charter (the protection from unreasonable search and seizure)

194. The majority decision found that while "there is no question that the taking of bodily samples for DNA analysis without the person's consent constitutes a seizure within the meaning of s.8 (per Charron J at para 25.), it was nevertheless reasonable. In reaching this decision heavy emphasis was placed on the safeguards inherent to the data bank regime and it was held that the current data bank provisions struck an appropriate balance between public

interest in the effective identification of persons convicted of serious offences, and the rights of individuals to physical integrity and privacy.

195. Charron J stated (at para 11):

> "a) A DNA data bank authorization must be obtained on **written application to a provincial court judge**. The judge is required to consider specified criteria in determining whether a DNA data bank authorization should be granted.
>
> b) The class of persons against whom a DNA data bank authorization may be granted is confined to a **specified class of convicted violent offenders**: s. 487.055(1), *Criminal Code.*
>
> c) Bodily **samples** collected pursuant to a DNA data bank authorization
> may only be used for **forensic DNA analysis** for inclusion in the National DNA Data Bank. **Unused portion**[s] of bodily samples are required to be **safely stored** at the National DNA Data Bank: s. 487.08(1), *Criminal Code*.
>
> d) It is a **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: ss. 487.08(2) and (3), *Criminal Code*.
>
> e) Use of DNA profiles and bodily samples at the National DNA Data
> Bank is **strictly limited to the narrow purposes of comparing offender profiles with crime scene profiles**. Any use of stored information or bodily samples or communication of information they may contain is strictly limited to the narrow identification purposes of the Act. **Access to the bank is restricted**. **Breach of any of those provisions is a hybrid offence subject to a maximum penalty of two years imprisonment** when prosecuted by indictment: sections 6(6), 6(7), 8, 10(3), 10(5), 11, *DNA Identification Act*.
>
> f) Communication of information as to whether a person's DNA profile
> is contained in the offenders' index may only be made to appropriate law
> enforcement agencies or laboratories for investigative purposes or to authorized users of the RCMP automated conviction records retrieval system: s. 6, *DNA Identification Act*.
>
> g) Although the seized **bodily samples are retained for safekeeping** in the DNA data bank, they **may only be used for further forensic DNA analysis where that is made necessary by "significant technological advances**" since the time that the original DNA profile

was derived. The results of such subsequent DNA analysis and any residue of the bodily sample are **subject to the same rigid controls** as the original profile and sample: s**. 10, *DNA Identification Act***.

h) Where a DNA profile cannot be derived from a bodily substance obtained during the execution of a DNA data bank authorization, further
samples may only be taken upon further authorization from a judge: s. 487.091, *Criminal Code*.

i) A DNA Data Bank **Advisory Committee** has been established by regulation. The composition of the Committee is stipulated as: a Chairperson, a Vice-Chairperson, a representative of the Office of the Privacy Commissioner and up to six other members who may include **representatives of the police, legal, scientific and academic communities**.

Retired puisne Justice Peter Cory of this Court is one of two representatives of the legal community on the current Committee. The
Committee's duties encompass "any matter related to the establishment
and operation" of the Data Bank upon its own motion or at the request of
the Commissioner. The Committee must report annually to the Commissioner: *DNA Data Bank Advisory Committee Regulations*, SOR/2000-181.

j) The Commissioner of the RCMP is required to report annually on the
operation of the National DNA Data Bank: s. 13.1, *DNA Identification Act*.

k) The *DNA Identification Act* is **expressly subject to a review of its provisions and operation by Parliament after five years**. That review is anticipated in the fall of 2005: s. 13, *DNA Identification Act*.

l) The Act permits sharing **of DNA profiles (but not stored bodily samples) with foreign governments and international organizations but only for legitimate law enforcement purposes** pursuant to specific
agreement or arrangement between the government of Canada and the
foreign government or international organization: s. 6(4), *DNA Identification Act*. Regulations under the Act further require that such agreements or arrangements "shall include safeguards to protect the privacy of the personal information used or disclosed under it": *DNA Identification Regulations*, SOR/2000-300." (Emphasis added throughout.)

196. The requirement of judicial authorisation was also considered in greater detail by Charron J (para. 51):

> "(1) prior judicial authorization must be obtained on written application to a provincial court judge: s. 487.055(1);
>
> (2) the applicant must establish that the targeted offender falls within one of the designated categories of offenders;
>
> (3) the judge has the discretion to give notice to the offender affected by the application;
>
> (4) the judge has the discretion not to order DNA sampling;
>
> (5) in deciding whether to grant the authorization, the judge is statutorily required to "consider the person's criminal record, the nature of the offence and the circumstances surrounding its commission and the impact such an authorization would have on the privacy and security of the person": s. 487.055(3.1);
>
> (6) the judge may require conditions to ensure that "the taking of the samples . . . is reasonable in the circumstances": s. 487.06(2); and
>
> (7) the police must report back in writing to the provincial court judge: s. 487.057(1)."

197. As only individuals convicted of designated offences came within these provisions of the Act, it was held that persons such as the appellant, who was a multiple sex offender, could not reasonably expect to retain any degree of anonymity after their conviction; his identity had become a matter of state interest and he has lost any reasonable expectation of privacy in the identifying information derived from DNA sampling in the same way as he has lost any expectation of privacy in his fingerprints, photographs or any other identifying measure (per Charron J, at para 43)

198. The dissenting judgement in *Rodgers* was led by Fish J (at paras 67 to 99) whose primary grounds for dissent was the fact that judicial orders for the seizure of DNA from convicted offenders could be made *ex parte* under the provisions of the *Code*, which he deemed unreasonable. He was critical of the databank and the power of the Government to seize DNA, despite the

requirement of judicial authorisation, pointing in particular to the fact that the DNA data bank constitutes a "substantial and novel invasion of privacy", and that specific offenders remain in the data bank for life. (per Fish J at para 95).

(c) United States

199. In the US, the Federal Bureaux of Investigation (FBI) operates the national Combined DNA Index Systems (CODIS) database. CODIS connects the 175 crime laboratories and the DNA databases of all 50 states, the US Army, the FBI and Puerto Rico.

200. The statutory basis for CODIS is the United States DNA Identification Act 1994. It originally provided only for the DNA of convicted offenders to be entered onto its offender index and it operated only on a prospective basis. In 2000 the DNA Analysis Backlog Elimination Act 2000 extended the provisions of the DNA Identification Act 1994 by providing for the collection and analysis of DNA samples from certain violent and sexual offenders for use in CODIS, and for inclusion in CODIS of DNA analyses of samples from crime scenes. The relevant offences include murder, voluntary manslaughter, sexual abuse, child abuse, kidnapping, robbery and burglary, and apply to those in jail, on parole, probation or supervised release to provide federal authorities with a "tissue, fluid, or other bodily sample" for the purpose of DNA analysis (U.S.C.S. 14135a(a)(1)-(2), (c)(1)-(2)).

201. In 2001 the Patriot Act added acts of terrorism to the list (USA PATRIOT ACT § 503, 115, Stat. 272, 364 (2001)).

202. Until 2004 DNA samples could only be taken from those convicted of certain serious or violent offences. The compatibility of the old law with the Fourth Amendment was challenged several times, as discussed below in relation to *US v. Kincade.* The constitutionality of the old law was ultimately upheld, with notable emphasis placed on the fact that it only applied to convicted offenders who had a 'reduced expectation of privacy'. However the Circuit Appeal Courts were invariably split, with dissenting judgments which criticised the retention of samples from even convicted offenders.

203. In October 2004 the 'Justice for All Act' allowed for an expansion of CODIS removing the restriction that only offenders charged with a serious or violent offence were required to provide DNA samples. However the statutory provisions governing the use and retention of samples and profiles on the expanded CODIS vary from state to state. A number of states have introduced legislation to require DNA from all convicted felons (Maine is the latest having just introduced this legislation in 2007).

204. Local, state and federal law enforcement agencies contribute samples to CODIS and the profiles are added to the database. This is trawled for matches against crime scene samples. DNA profiles in CODIS are organised in two indices, as in the Canadian database: the Forensic Index (profiles obtained from crime scene evidence) and the Offender Index. The Offender Index contains DNA profiles of individuals collected under applicable federal, state or local laws.

205. In January 2007 CODIS contained 4,274,700 DNA profiles. Over 4 million of these profiles were from persons convicted of serious or violent offences.

206. There is a variable policy concerning retention of samples in the US: some State laboratories retain them whereas others destroy them.

207. The operation of CODIS is subject to external monitoring and auditing by the Department of Justice Office of the Inspector General. An audit by the Inspector General was conducted in 2001 and contained criticisms relating to the FBI's oversight of CODIS-participating laboratories.

208. The CODIS system is overseen by an external public advisory committee that consists of experts in ethics and a Supreme Court judge.

Compatibility with the Fourth Amendment

209. The Fourth Amendment to the U.S. Constitution states:

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

210. It is well established in US case law that the collection of a saliva sample for DNA analysis is a search implicating the Fourth Amendment (*Groceman v U.S. Dep't of Justice*, 354 F.3d 411, 413 (5th Cir. 2004)). Furthermore the Court has expressly recognised that the initial procurement of a biological sample and the subsequent analysis of the sample are two conceptually distinct

events necessitating independent Fourth Amendment analyses: *Skinner v Ry. Labor Executives Ass'n* 498 US 602, 616, 618 (1989).

Retention of Samples from Convicted Offenders

211. The provisions for retention of DNA samples and profiles from convicted offenders was the subject of constitutional challenge in *United States v Kincade*, 379 F 3d 813, 833-36 (9th Cir. 2004), in which a parolee who was not suspected of committing any further offences objected to the requirement that he provide a DNA sample on the basis that it was a violation of the Fourth Amendment.

212. The Court in *Kincade* upheld the constitutionality of the Act by a narrow majority (6-5) on the basis that as only convicted offenders who had been proven guilty of a crime were bound to provide DNA samples, the government had a heightened legitimate interest in monitoring them and hence the individuals concerned a diminishing expectation of privacy. This amounted to a 'special needs' test which overrode the balancing requirements of the utility of the measures weighed against an individual's right to privacy.

213. Delivering the majority opinion O'Scannlain J said that the public interest served by collecting DNA outweighed parolees' "substantially diminished expectations of privacy" and "the minimal intrusion occasioned by blood sampling." (*Kincade,* per O'Scannlain J.)

214. However, the question as to when samples and profiles so obtained should be destroyed was left open, with an acknowledgment that this would be an

important question for a future court to decide. Gould J concurring emphasized that the court had not determined the rights of an individual "who has fully paid his or her debt to society, who has completely served his or her term, and who has left the penal system" and asked, "Once those previously on supervised release have wholly cleared their debt to society, the question must be raised: 'Should the CODIS entry be erased?" Judge Gould noted that this question would have to be addressed in a future case.

215. Reinhardt J's dissent, joined by Pregerson J, Kozinski J, and Wardlaw J, spoke strongly against the erosion of privacy represented by the majority decision:

> "Never has the [Supreme] Court approved of the government's construction of a permanent governmental database built from general suspicionless searches and designed for use in the investigation and prosecution of criminal offenses."
>
> Privacy erodes first at the margins, but once eliminated, its protections are lost for good, and the resulting damage is rarely, if ever, undone. Today, the court has opted for comprehensive DNA profiling of the least protected among us, and in so doing, has jeopardized us all."

216. Kozinski J emphasised the relative urgency of clearly defining the limits of the expanding database (*U.S. v Kincade,* 379 F.3d at 873):

> "Later, when further expansions of CODIS are proposed, information from the database will have been credited with solving hundreds or thousands of crimes, and we will have become inured to the idea that the government is entitled to hold large databases of DNA fingerprints. This highlights an important aspect of Fourth Amendment opinions: Not only do they reflect today's values by giving effect to people's reasonable expectations of privacy, they also shape future values by changing our experiences and altering what we come to expect from our government. An opinion…that draws no hard lines and revels in the boons that new technology will provide to law enforcement is an invitation to future expansion".

217. A case currently pending in the Supreme Court, *Johnson v Quander,* raises a further challenge to the provisions for warrantless suspicion-less seizures of DNA from individuals on probation. The case concerns the appellant being asked to provide a DNA sample shortly before the completion of his two-year probationary period, pursuant to the DNA Analysis Backlog Elimination Act 2000. The appellant claims that these amount to a violation of the Fourth Amendment, and the International Convention of the Elimination of All Forms of Racial Discrimination ("CERD").

218. On 17th March 2006 the D.C. Circuit rejected the claim, on the basis that a probationer had a lowered expectation of privacy and that the compulsory production of a blood sample was a "reasonable" search under the Fourth Amendment, since it furthered a government interest--identifying recidivist criminals - that was greater than Johnson's privacy interest in keeping his identity secret. *Johnson v Quander*, 440 F.3d at 496. However this approach was based on those who have paid their debt to society having greater privacy interests than those still in custody; it was stated that privacy interests are not fully restored to their pre-conviction level and are not intended to be equal to the interests of those never convicted of a felony. This suggests by implication that those never convicted of a felony have higher rights of privacy that would not necessary justify the retention of their genetic identity.

Provisions relating to suspects

219. The 2004 'Justice for All' Act allowed for an expansion of CODIS to suspects; section 203 of the 2004 Act significantly expands CODIS, so that a State can include virtually any DNA information it chooses, including that of uncharged

arrestees and voluntary samples for elimination purposes, and from all previously convicted offenders.

220. Further, in 2005 the Violence Against Women Act was amended to authorise the collection of DNA samples from individuals who are arrested or detained by federal authorities - even if they are not convicted, or charged with a crime.

221. Some US states have now introduced legislation requiring DNA sampling of certain categories of arrestees. California's 'Proposition 69' was the first to do so, introducing compulsory DNA sampling of all individuals either arrested on suspicion of or charged with certain violent offences, namely murder, voluntary manslaughter, or a felony sexual offence (and all persons who have ever been arrested for those offences).

222. The Minnesota Court of Appeal has held such provisions to be unconstitutional. In *State of Minnesota, Court of Appeals, A06-874, In the Matter of the Welfare of: C.T.L., Juvenile,* the court struck down a state law authorizing the warrantless, automatic collection of DNA samples from people charged with but not convicted of crimes, on the grounds that the privacy interest of a person charged but not convicted is not outweighed by the state's interest in collecting and analyzing a DNA sample.

223. In a similar case, *Kohler v. Englade,* US Court of Appeal Fifth Circuit, No. 05 –30541 (21st November 2006) the Court found that the seizure of DNA from the appellant as one of 600 suspects in a serial killing investigation, pursuant

to a warrantless, suspicionless DNA dragnet, was unconstitutional and lacked probable cause. The appellant had refused to provide DNA, and a warrant authorised by a magistrate had then been issued compelling him to provide a sample. It was held necessary to show probable cause before a warrant authorising compulsory DNA sampling could be justified under the Fourth Amendment.

224. Although the case did not consider the wider privacy implications of DNA samples and profiles being, it does emphasise the need for thorough judicial scrutiny of decisions to obtain DNA samples from those suspected of, but not convicted of, committing an offence, and the constitutional requirement that any such decisions must be founded on probable cause.

Retention of Samples

225. In relation to individuals convicted of an offence, but whose conviction is overturned, the DNA Identification Act explicitly provides for expunge of the profile if the director of CODIS receives a certified copy of a final court order establishing that the conviction has been overturned. The Act is otherwise silent on the question of destruction of DNA samples.

226. Individual states tend to have no statutory provisions governing whether the sample should be retained or destroyed. Five states mandate that officials automatically eliminate innocent individuals' samples from state databanks when proceedings against them have been discontinued. California permits a

person to make a written request for expungement of DNA profile and destruction of sample if:

a. He is arrested but no accusatory pleading filed on time;
b. He is arrested but charges dismissed; acquitted, or found not guilty; or
c. The underlying conviction is reversed or case dismissed.

The court has discretion whether to grant the expungement or not: California Penal Code § 299(b)(2005).

227. Wisconsin's statute requires the destruction of samples once a DNA profile has been generated.

228. In relation to convicted offenders, New Jersey has held that DNA samples and records 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. This ruling was based on the fact that once an ex-felon has fully completed his sentence, his privacy expectations increase, and at the same time, the Government's justifications for maintaining the DNA profile decline.. It further held that once one's debt to society was paid "permanently retaining a former offender's seized DNA in a state database is somewhat akin to the government keeping his property without a forfeiture hearing or a waiver of an interest in that property": *A.A. v Attorney General,* at 55.

(d) Australia

229. In Australia there are two databases for law enforcement purposes. These are the Australian Federal Police Database and the National Criminal

Investigation database (NCIDD system). The Australian Federal Police Database is the Police's own internal database. The NCIDD system aims to encourage inter-jurisdictional matching of DNA profiles.

230. CrimTrac is the agency responsible for operating the NCIDD system. The Australasian Police Minster's Council defines CrimTrac's policies and appoints members to its board of management.

231. The oversight afforded under the current regime was condemned by the Australian Law Reform Commission as insufficient in a 2003 Report, and the Government responded by determining that oversight should move to an independent model, as recommended by the HGC for the United Kingdom a year earlier.

232. Following the 2003 Report Victoria conducted a review of its system and published a report, *The Victoria Parliament Law Reform Committee, Forensic Sampling and DNA Databases in Criminal Investigations* (Melbourne VPLRC, 2004). The report rejected the introduction of a scheme comparable to that in the United Kingdom and held (p. 230):

> "From a public policy perspective, the Inquiry sees the current system of court orders as affirming a connection between the taking of the sample and its forensic utility in a specific investigation. This serves to ensure that the primary purpose of DNA sampling of suspects remains the detection of offences for which they have already been identified as suspects."

233. The Victoria statutory scheme (under the Crimes Act 1958 (Vic) as amended by the Crimes (DNA Database) Act 2002) requires police to obtain a judicial

warrant before a non-consensual DNA sample can be taken from a suspect, provides for samples to be taken only from a person suspected of a narrow range of offences and in circumstances where the sample if obtained would tend to confirm or deny involvement in a crime. Samples and profiles which are taken are only to be retained for a period of twelve months from the taking of the sample. It was recommended in the Report that this system be retained as:

> "The Committee believes it is desirable to require the destruction of the sample as soon as practicable after the profile has been obtained. Should a second sample be required for verification purposes, a second procedure can be obtained" (Recommendation 4.4).

234. The Victorian system, despite its limited scope, has nevertheless been heavily criticised in Australia, principally on the grounds that convicted offender profiles are retained indefinitely, regardless of whether the individual is a recidivist; the fact that suspects' profiles for 12 months, and the broadening of the relevant offences to those carrying a maximum sentence of five years imprisonment or more.[8]

(e) New Zealand

235. In some respects, the New Zealand National DNA Databank is comparable to the NDNAD of England and Wales, as it combines volunteer and convicted criminal DNA. However, there the similarities end, as compelled DNA is limited to those convicted of serious offences, samples are immediately destroyed upon generation of the profile for the Databank and there are relatively strong privacy safeguards in place.

[8] Gregory Gardiner, 'Racial Profiling: DNA Forensic Procedures and Indigenous People in Victoria', Crim. Just. 47 2005 - 2006

236. In 1995, the New Zealand Police worked with a private scientific company to establish the databank. The concept involved the collation of DNA profiles from convicted offenders *and* volunteers on a central Database to be administered by ESR (the private company) on behalf of the New Zealand Police. This database was to be challenged with DNA profiles obtained from unsolved crimes in an attempt to identify any individual(s) linked to a particular offence through biological material from the crime scene or investigation.

237. The Criminal Investigations (Blood Samples) Act 1995 was passed to facilitate the creation of the databank. The 1995 Act was formulated after considering representations from members of the police, legal and scientific communities. The Act was designed with a strong focus on the rights of the individual and places strict requirements on police investigators obtaining blood samples and ESR as custodians of the Databank.

238. The Act took effect on 12 August 1996 and covers in detail the submission of reference blood samples from the following four categories of person:

(a) suspects in any criminal investigation who volunteer a reference blood sample for comparison with that particular investigation and/or inclusion on the DNA Databank;

(b) all persons convicted of a relevant offence for which a Databank request is made;

(c) any individual who volunteers a blood sample to be included on the DNA Databank;

(d) suspects and/or Databank samples which are obtained by compulsion.

Category (d) above was expanded in 2004 to include all criminals convicted of an offence carrying a sentence of seven or more years.

239. Individuals who submit blood samples to the DNA Databank are asked to voluntarily provide detailed ethnic information which indicates ancestry over a period of four generations. This provision has been included in the Act to enable ESR to compile accurate sub-population data for statistical use within New Zealand.

240. Issues such as security, confidentiality, disclosure, sample storage and destruction and deletion of samples are also addressed in detail in the Act.

241. Blood sampling kits are provided to the New Zealand Police to facilitate the collection of whole blood or finger-prick samples. All contents of each kit are labeled with a unique six digit barcode. These barcodes are used as unique identifiers for the samples as they move through the various stages of analysis, including loading to the Databank itself.

242. Since the operational beginning of the Databank in 1996, over 64,000 individual profiles have been added to the Databank. Approximately 800 to 1000 profiles a month continue to be added.

243. Once DNA profiles are generated the DNA sample is destroyed for privacy reasons.

V. Fingerprint Databases in Common Law Countries

244. 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.

245. 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.

246. Further, in most common law countries computer data attached to the fingerprints is also destroyed if the individual is not subsequently convicted, or, at the very least, access to such data is strictly controlled.

247. There is extensive Canadian jurisprudence concerning fingerprint collection, retention and use. In a series of cases the Canadian courts have examined the related questions of whether there is an interference with the right to privacy

when lawfully obtained fingerprints are obtained for a particular purpose, and then either used in a manner which exceeds that purpose, or retained for a different purpose. They have concluded that there is a *prima facie* interference in such cases (and it then falls to the State to justify that interference).

248. This first arose in *R. v. Colarusso* (1994) 87 CCC (3d) 193 (Supreme Court of Canada), a case in which the accused had caused a fatal car accident. Blood and urine samples were taken from the accused at the hospital with his consent by the medical staff. The coroner required those samples in connection with the investigation of the death of the accident victim and obtained them from the hospital lab under statutory authority of the Coroner's Act 1980. The coroner delivered the samples to the police to take to the forensic testing centre for analysis. At trial, the Crown called the forensic analyst to report the blood alcohol level of the accused based on the forensic tests of the blood and urine samples which had been obtained by the coroner. A majority of the Court held that when the police took the samples that constituted a seizure of the samples from the coroner and that a warrantless seizure was unreasonable and therefore contrary to s. 8 of the Charter. The majority found that it was also possible to take the view that the actions of the police made the originally valid seizure by the coroner unreasonable, since the evidence from that seizure was appropriated by the police for law enforcement purposes that went beyond the limited purpose for which the coroner was statutorily authorized to take the samples. On this issue, La Forest J made the following comment (p. 222):

> "Once the evidence has been appropriated by the criminal law enforcement arm of the state for use in criminal proceedings, there is no foundation on which to argue that the Coroner's seizure continues to be reasonable. In considering this position, it must be understood that the protection against

> unreasonable seizure is not addressed to the mere fact of taking. Indeed, in many cases, this is the lesser evil. Protection aimed solely at the physical act of taking would undoubtedly protect things, but would play a limited role in protecting the privacy of the individual which is what s. 8 is aimed at, and that provision, *Hunter* tells us, must be liberally and purposively interpreted to accomplish that end. The matter seized thus remains under the protective mantle of s. 8 so long as the seizure continues."

249. In the case of *R. v. Dore* [2002] 162 OAC 56, (2002) 166 CCC (3d) 225 (Ontario Court of Appeal) the court examined *Colarusso* and the subsequent cases of *R. v. Borden* (1994), 92 CCC (3d) 404 (SCC), and *R. v. Arp* (1998), 129 CCC (3d) 321 (SCC). Both *Borden* and *Arp* considered the narrow question of whether there had been a waiver of the right to be free from unreasonable searches and seizures (s. 8 of the Charter) when bodily samples were given with consent for the purpose of one investigation but then used in a second investigation, and whether the original consent could be said to have extended to permit that use.

250. *Dore* concerned the question of whether the retention and use of the appellant's fingerprints after criminal charges against him were withdrawn constituted an unreasonable search and seizure contrary to s. 8 of the Charter, and consequently, an unconstitutional retention and use of the fingerprints. Feldman JA described the correct approach in assessing the lawfulness of such retention as follows (paras. 37, 38):

> "In this case the constitutional attack is on the retention of the fingerprints rather than on any subsequent seizure. As affirmed in *Colarusso* and subsequent cases, the "protective mantle" of s. 8 extends during the duration of the holding and retention of the thing seized in order to protect the privacy interest of the person from whom it was seized. Consequently, if the constitutional safeguards that were present and justified the seizure are no longer in place, then unless they are replaced by new constitutionally accepted safeguards, the retention as an ongoing seizure may become unreasonable and no longer justifiable.

> In order to determine whether and if so at what point an acquittal or discharge on the original charge which allowed the police to take the fingerprints makes the ongoing retention and use of those fingerprints an unreasonable seizure, the court must undertake a traditional s. 8 analysis." (Paras. 37 and 38.)

251. Feldman JA set out three questions for the state to answer:

(a) is the ongoing retention authorised by law?

(b) is the law reasonable? and

(c) is the retention in this case reasonable?

252. On question (a) ('is the ongoing retention authorised by law?') Feldman JA concluded that some retention was authorised by law due to the wording of the relevant statute, but the extent of that statutory authorisation is subject to a reasonableness analysis.

253. On question (b) ('is the law reasonable?') he detailed that the objective of s. 8 of the Charter is to protect the individual's reasonable expectation of privacy. He concluded that, from the privacy point of view, there are two aspects of a "seizure" of fingerprints. The first is "the actual physical act of taking the impression of the fingers, including the physical and psychological indignity involved in that process" (para. 47). The second is "the acquisition by the state of the informational component of the fingerprint, its unique characteristics and identifying relationship to the particular individual" (para. 47). He continued:

> "Once fingerprints have been taken from an individual, it is only the informational component of the fingerprint about which a person can retain any expectation of privacy. When a person continues to be subject to the charge for which the person was arrested, or has been convicted of the charge, then the original basis for obtaining the information disclosed by

> fingerprints set out by La Forest J. in *Beare* and *Higgins* continues and therefore justifies the retention and use of that information on an ongoing basis for law enforcement purposes.
>
> But once the original justification has been removed, is there any basis for viewing the privacy interest of such a person in his or her fingerprint information, whatever that interest may be, as any different from that of any other innocent person in society? Does an acquitted person have a reduced expectation of privacy in that information?
>
> …In my view, anything associated with one's body, especially where it is not something that is otherwise normally accessible, is of a personal and confidential nature and is the type of information that people expect to be able to control and keep private in the ordinary course. The fact that one's fingerprints may tell nothing about the person other than his or her identity hardly makes the information impersonal.
>
> Linked to the inherent privacy interest one has in anything emanating from one's body, is the factor that the fingerprints are stored by the police because they were originally obtained under the *Identification of Criminals Act*. Therefore, the storage and use of the fingerprints is associated with the identification of the person as a criminal, when the person has not been convicted of the offence. Some U.S. courts identified this "rogues gallery" problem in early cases on the privacy interest… This concern was also identified by the Saskatchewan Court of Appeal in *Beare* and *Higgins* as a serious problem with retention (the issue not dealt with by the Supreme Court).
>
> One argument made against a privacy interest in fingerprints is that fingerprints are not inherently incriminating, but only become incriminating when linked to the scene of a crime: see: *R. v. Connors* (1998), 121 C.C.C. (3d) 321 at 389-90 (B.C.C.A.). In my view, this concept adds nothing to the debate on whether a person has a privacy interest in his or her fingerprint information. The same can be said about DNA: it is also not inherently incriminating, but this does not speak to the privacy interest one may have in its contents, including its ability to identify a person.
>
> Finally, the practice in some other common law countries reflects a recognition that an acquitted person may well retain an interest in maintaining the privacy of fingerprint information. The fact that such countries as Scotland, New Zealand, Tasmania and several states of the United States have enacted legislation providing for the destruction or return of an individual's fingerprints upon acquittal or withdrawal of charges suggests that such a privacy interest may remain when a person is effectively cleared of the offence for which the fingerprints were taken" (Paras. 50, 51, 53, 54, 55, 59.)

254. Feldman JA briefly and dismissively referred to the contrary finding in the Divisional Court of England and Wales in *S and Marper*, and stated that (para. 64),

> "There is not basis in the case case law or otherwise, to infer that a person who was subjected to fingerprinting upon arrest will not have some reasonable expectation of maintaining or regaining his or her privacy in fingerprint information if the charge is disposed of in his or her favour. There is no reason to differentiate the expectation of privacy that an acquitted person has in such information from the expectation that a person who has never been charged with an indictable offence would have, because it is information about and from one's body not normally available without one's consent. Added to that in the context of retention is the nature of the storage by the police which tends to stigmatize as a criminal the person whose fingerprints are retained. Although it may be that because of the nature of that information, the expectation of privacy is minimal when compared, for example, to information which can disclose the genetic make-up of the person and not merely the person's identity, I conclude that a person can have some privacy interest in the retained fingerprints."

255. Finally, Feldman JA considered question (c) ('is the retention in this case reasonable?'). He noted that it is possible for retained fingerprints lawfully obtained for the investigation of a particular offence to violate s. 8 of the Charter. However, he considered the Canadian system of destroying such fingerprints if requested to do so by the acquitted person to strike a 'fair balance' between the interests of the individual and those of the state. At para. 72 he stated that,

> "The fact that the police have a practice of destroying fingerprints when requests are made by persons where the charge has been disposed of in their favour is significant evidence that such a request tips the balance in favour of the privacy interest."

256. The policy of destruction on request (the pre-2001 English and Welsh system) was considered sufficient to protect the privacy interest, in the totality of the circumstances. In this particular instance retention had been reasonable as the individual had not requested destruction of the prints.

E. DOMESTIC PROCEEDINGS

257. The following does not represent an exhaustive analysis of the domestic decisions, but does raise distinct points not addressed elsewhere.

I. Factual Errors

258. The three levels of judgment within the domestic courts (Divisional Court, Court of Appeal and House of Lords) contained many factual inaccuracies, in particular concerning how the NDNAD works in practice, how it interacts with PNC and the distinction between DNA samples and DNA profiles.

259. On 22 March 2002 the judgment of the Divisional Court was given by Leveson J., when sitting with Lord Justice Rose, Vice-President. At paragraph 6 of the judgment Leveson J. states:

> "It is important to appreciate that the DNA database is not a list of suspects; rather, it will show only a 'hit' of a DNA profile of an individual which matches that from DNA recovered at a crime scene."

Leveson J.'s understanding of the operation of the NDNAD, as revealed in this paragraph, is flawed. The NDNAD does constitute a list of suspects and convicted criminals, with the biographical information (name, address, date of arrest, suspected or confirmed offence) concerning those individuals listed on the PNC rather than the NDNAD itself. The corollary of being on the NDNAD is that one will also appear in a list of suspects and criminals on the PNC; in fact, it is not possible to create an NDNAD record without the PNC record. This NDNAD/ PNC link was not appreciated by the Divisional Court and the confusion persisted in the Court of Appeal and the House of Lords. The system described by Leveson J. (an anonymous system until a 'hit' is made) is precisely the type of system the Information Commissioner's Office (ICO) argued for (see attached letter CG2) as they believed this was the only privacy-compatible means of retaining

such information following the individual's exoneration by the courts or the dropping of charges against him. However, the Government did not follow the ICO's advice and the current system was put in place.

260. At paragraph 19 Leveson J. states his doubts concerning whether Art. 8(1) is engaged because:

> "A person can only be identified by fingerprint or DNA sample either by an expert or with the use of sophisticated equipment or both; in some cases, it is essential to have some sample with which to compare the retained data."

There are a number of problems with this point of Leveson J.'s. First, the sophistication of equipment or the level of expertise required to access sensitive, personal information does not detract from its private quality. A compulsory blood test, for example, is not a less private issue because it requires 'sophisticated' scientific equipment to analyse results (*X v. Austria*, 18 DR 154 (1979), E. Commission on Human Rights). In assessing Art. 8(1)'s applicability to information retained by the State the means of access to that information is irrelevant (although it may, of course, be relevant to the question of whether the interference is justified under Art. 8(2) ECHR). Second, Leveson J.'s suggestion that identification of the individual is difficult and, when possible, limited to 'experts,' is not sustainable. The data retained is not simply the fingerprint, DNA profile or DNA sample; the biographical information which is necessarily retained to identify the provenance of such material means that a person can be readily identified from his or her PNC record. Such information can be accessed by police officers at any level at any police station nationwide, customs officials, other public officials, and even certain private groups. The lengthy list of bodies with access to the PNC is attached as CG1. This identification of the individual from his or her PNC record hardly requires 'sophisticated' equipment, unless Leveson J. would classify a computer terminal as such.

261. Paragraph 19 of Leveson J's was repeated in both the Court of Appeal (para. 33) and the House of Lords (para. 29) with no correction of the factual error concerning access to information. Again, it was assumed that information on the NDNAD is virtually inaccessible without a 'match' between a profile and a crime scene sample, and the availability of such information on the PNC was not acknowledged.

262. Paragraph 19 of Leveson J's judgment in the Divisional Court continues:

> "Further in the context of the storage of this type of information within records retained by the police, the material stored says nothing about the physical makeup, characteristics or life of the person to whom they belong."

This is a surprising argument. Leveson J. appears to argue that because the PNC record does not contain "physical makeup" information, "characteristics" information or information concerning the "life" of the person Art. 8(1) is not engaged, despite the fact that identifying information, such as name and address, and information relating to a past suspicion of involvement in an offence is retained on the PNC record. There is no basis for this claim in the Art. 8 case law of the Court.

263. In the House of Lords the lack of awareness of the interaction between the PNC and the NDNAD and, in particular, the absence of evidence concerning abuse and misuse of the system appears to have contributed to Lord Brown's dismissal of the appeals. At para. 86 he states:

> "Given the carefully defined and limited use to which the DNA database is permitted to be put—essentially the detection and prosecution of crime—I find it difficult to understand why anyone should object to the retention of their profile (and sample) on the database once it has lawfully been placed there."

(Again, there is an incorrect assumption that the DNA sample is retained on the NDNAD, rather than simply the profile.) At para. 87 Lord Brown dismisses as 'unrealistic' the notion that individuals such as the Applicants might be stigmatised or disadvantaged through the retention of their information.

264. It is clear that individuals whose information is retained are stigmatised in four main ways:

(a) general 'soft' discrimination (the use of language such as 'active criminal population,' 'offenders' database' and 'criminal database' in official, quasi-official and general parlance.);

(b) structural discrimination in the process (contrast the safeguards attached to the Police Elimination Database and its inbuilt presumption that the police do not commit crimes with the NDNAD and NAFIS, and their attachment to 'criminal records' on the PNC);

(c) 'hard' discrimination (e.g. information being released to the CRB which results in future employers being told about arrest information, and 'enforced subject access' requests);

(d) racial issues and familial issues (the database is self-perpetuating and the existing over-representation of certain ethnic and other groups is increasing exponentially (i) as the over-representation of certain races spills into racial profiling, and (ii) with familial searching the families of individuals already on the database are then added as volunteers).

265. At all three levels in the domestic courts the distinction between DNA samples and DNA profiles was blurred, and the fact that DNA samples are not used for forensic purposes following the generation of the profile was not recognised. Lord Steyn in the House of Lords at paras. 7 and 8, for example, spoke of the value of DNA evidence in the following terms:

> "**The value of retained fingerprints and samples** taken from suspects who were subsequently acquitted is considerable. This is graphically illustrated by a real case which has been referred to as "I". In 1999 a rape and robbery took place. The perpetrator was not known to the victim. DNA was recovered from the semen on the victim. A search of the national database showed that the DNA matched that of "I". **The sample should have been destroyed. It was not**. Following the decision of the House of Lords in *Attorney-General's Reference (No. 3 of 1999)* [2001] 2 AC 91 the prosecution went ahead. "I" pleaded guilty to rape and was sentenced to a term of seven years (subsequently reduced on appeal to six years) in a young offenders institution. **But for the wrongly retained sample** the offender might have escaped detention, possibly to commit other serious crimes" (emphasis added).

Referring to the value of the retained DNA *sample* when it played no part whatsoever in identifying "I" illustrates that Lord Steyn based his assessments on erroneous information. "I" was identified due to the retention of his DNA profile, and his sample was never accessed or used for investigative purposes. Lord Steyn's blurring of the sample/ profile distinction undermines his subsequent finding that not even the indefinite retention of samples engages Art. 8(1).

II Scope of Article 8(1)

266. The notion of 'private life' in Art. 8 ECHR is a broad one and is not susceptible to exhaustive definition: *Niemitz v. Germany* (1993) 16 EHRR 97; *Costello-Roberts v. UK* (1995) 19 EHRR 112. It is well-established that the categories of private life under the Convention range widely and encompass the right to *be* oneself, to *live* as oneself and to *keep* to oneself.

267. Throughout the twentieth century, privacy was primarily formulated as a negative claim. Such a formulation was again used by Geoffrey Robertson in 1993, who posited that the right to privacy is, at its most basic and generic, "the right to be able to live some part of life behind a door marked 'do not disturb'" (*Freedom, the Individual and the Law*, 1993). During that century different definitions moved from a negative claim towards more positive rights. Many of these positive formulations were based around the notion of privacy *qua* autonomy and freedom in decision-making. However, many commentators who deal with informational privacy alone have also outlined positive formulations of informational privacy, viewing it as a freedom from *and* a freedom to, a right to informational self-determination in both a positive and negative sense. This view considers freedom of information and data protection rights to be subsets of the same general right to control the flow of information about ourselves, to be able to communicate the information or keep it for ourselves alone.

268. Art. 8 ECHR is notionally divided into separate categories: the right to respect for private life; the right to respect for family life; the right to respect for home; and, finally, the right to respect for correspondence. These sub-categories often overlap and intermingle.

269. There are five aspects of privacy now accepted in international and comparative jurisprudence, and these five aspects underpin the Art. 8 case law of the European Court of Human Rights. Again, they are not mutually exclusive and often overlap with each other.

(i) Bodily or Physical Integrity

270. Physical privacy is almost never referred to as such: it is concerned with the protection from outside interference of the body, the physical self. Physical privacy is widely protected in most democratic countries through both the criminal and civil law (rape, assault, battery, and so on). However, many issues which fall within

its remit are not always adequately legally covered: excessive strip-searching, genetic testing, biometric testing, drug testing and cavity searches.

271. Physical integrity is, in the main, protected through the Court's jurisprudence on 'private life': unnecessary handcuffing by the military authorities for persistent refusal to undergo military service is within the remit of Art. 8(1) (*Raninen v Finland* (1997) 26 EHRR 563); compulsory blood tests in paternity proceedings is also within its remit (*X v Austria*, 18 DR 154 (1979)); as is excessive force used in a private home by the child's step-father (*A v UK* (1998) 5 BHRC 137).

272. Article 8(1) also encompasses impairments to physical well-being by non-physical assaults, such as pollution (*Lopez Ostra v Spain* (1995) 20 EHRR 277 and *Guerra v Italy* (1998) 25 EHRR 357) and noise pollution (*Rayner v UK*, 47 DR 5 (1986)).

273. Further, Art. 8(1) incorporates positive duties on the state to protect a person's physical integrity: *X and Y v Netherlands* (1985) 8 EHRR 235 (the failure of domestic law to provide the right for a mentally handicapped person to bring a prosecution for sexual assault amounted to a failure to secure respect for her private life).

274. Inroads into physical privacy may involve subsequent inroads into informational privacy. This may occur, for example, if results of a biometric test are kept on a database or photographs of suspects are kept with identifiable information on a state file.

(ii) Informational Privacy

275. Informational privacy concerns the collection, use, tracking, retention and disclosure of personal information. It is often contrasted with decisional privacy, but informational privacy increasingly incorporates elements of decisional privacy as the use of data both expands and limits individual autonomy.

276. Informational privacy includes data protection, but it is broader than this, and also includes more 'positive' informational rights, such as freedom of information. It is, essentially, a right to informational self-determination. In the words of the now retired judge of the Canadian Supreme Court, La Forest J,

> "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).

These words echo those of Alan Westin, the renowned privacy scholar:

> "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (*Privacy and Freedom*, 1967).

277. Informational privacy is protected in Art. 8 ECHR primarily through the right to respect for private life and correspondence, although it is also protected through the right to respect for home and family life, depending on the facts of particular cases.

278. Jurisprudence relating to the concept of 'private life' has demonstrated that Art. 8 applies to informational privacy surrounding issues such as one's name, sexual orientation, identity and previous gender.

279. Jurisprudence relating to state interference with correspondence or communications is similarly broad, and Art. 8(1)'s reach in this regard covers issues such as enforced fingerprinting or photographing as part of a criminal investigation (*Murray v UK*), surveillance of the individual (*Klass v Germany* (1978) 2 EHRR 193), and collecting and retaining data about the individual (e.g. *Hewitt and Harman v UK* (1992) 14 EHRR 657 and *Chare (née Jullien) v France*, 71 DR 141 (1991)).

280. When dealing with genetic information in particular, informational privacy incorporates a 'right *not* to know'. The right not to know is based partly in informational privacy and partly in decisional privacy, or autonomy.

281. This right not to know is recognised in various international instruments, including the UNESCO Universal Declaration on the Human Genome and Human Rights and the Council of Europe Convention on Human Rights and Biomedicine.

(iii) Spatial Privacy

282. Spatial privacy (sometimes referred to as 'territorial privacy') concerns the setting of limits on intrusion into personal spaces. Spatial privacy is protected in Art. 8 ECHR not only via the protection of 'home,' but also 'private life'.

283. 'Personal spaces' may include not only the home and domestic environments, but also the workplace, one's car, and even public space, depending upon the context. This was recently confirmed by the Court in the admissibility decision in *Martin v. UK* (27 March 2003). The government had unsuccessfully argued that covert surveillance of the applicant's home by video camera was not an Article 8 issue as the nuisance which the surveillance attempted to address was not private in nature, and the camera only recorded what would have been visible to a neighbour or a passer-by on the street. The Court again confirmed this point in the recent case of *Von Hannover v. Germany* (Application number 59320/00, judgment handed down 24th June 2004).

284. Certain venues may, depending upon the legal system, carry with them a presumption that they are private spaces, e.g. bedrooms and bathrooms. Many common law jurisdictions with constitutional rights to privacy, for example, refer to the 'inviolability of the dwelling' (e.g. Ireland, US, Canada).

285. However, spatial privacy is not restricted to venues such as bedrooms and bathrooms, or even homes. "It is a kind of space that a man may carry with him, into his bedroom or into the street," as one commentator has put it (Konvitz, 'Privacy and the Law: A Philosophical Prelude' (1966) 31 *Law and Contemporary Problems* 272, 280).

(iv) Relational Privacy

286. Privacy includes the right to interact with others and to – insofar as is reasonable – govern those interactions. This is recognised in the case law of the European Court of Human Rights concerning 'private life,' 'family life' and 'correspondence'.

287. Relational privacy has a positive and a negative aspect: it includes both the freedom to associate with others (and determine the extent and nature of that association) and freedom from others. The positive aspect, the freedom to associate, is akin to Alan Westin's description of 'intimacy' as one of the states of privacy, and the negative aspect, freedom from others, akin to his description of 'solitude'. In addition, relational privacy in the positive sense, engaging with others, is often facilitated by anonymity.

(v) Decisional Privacy

288. Decisional privacy concerns the freedom to make decisions about one's body, one's self and one's family. In many jurisdictions with constitutional rights to privacy (enumerated or unenumerated) the term 'privacy' is used as shorthand for this idea, and it overlaps almost entirely with the concept of personal autonomy (the constitutional case law of Ireland and the US exhibits this trend).

289. Decisional privacy involves matters such as contraception, procreation, abortion, child-rearing, expression of one's sexual orientation, and suicide.

290. The NDNAD process engages many aspects of privacy. Physical integrity (both in the taking of the sample and retention of the sample and profile once its immediate purpose in a live criminal investigation has been served) and informational privacy are clearly engaged. However, decisional privacy and relational privacy are also engaged, as possible disclosure of retained information may affect the individual's ability to make decisions affecting his or her life, and his or her relationships with others. The combination of these different aspects of privacy is recognised by the Canadian Privacy Commissioner in his report on *Genetic Testing and Privacy* (1995, at p 2), quoted by Baroness Hale in the House of Lords in *S and Marper* (para. 69):

> "The measure of our privacy is the degree of control we exercise over what others know about us. No one, of course, has absolute control. As social animals, few would want total privacy. However, we are all entitled to expect enough control over what is known about us to live with dignity and to be free to experience our individuality.
>
> Our fundamental rights and freedoms - of thought, belief, expression and association - depend in part upon a meaningful measure of individual privacy. Unless we each retain the power to decide who should know our political allegiances, our sexual preferences, our confidences, our fears and aspirations, then the very basis of a civilised, free and democratic society could be undermined."

291. The type of information DNA reveals is profoundly private. Indeed, in many cases the information is so private that the individual himself may be unaware of it. DNA is not only revelatory concerning the individual whose DNA it is, but may be revelatory concerning the individual's relationship to others (whether his apparent father is his biological father, for example) and the propensity of his relatives to particular diseases. Far from being an 'insubstantial,' 'modest' or 'minor' Art. 8 issue, it is suggested that the material at issue in this case is 'a most intimate aspect' of private life (*Dudgeon v UK* (1981) EHRR 149, paras. 40 – 41 and 52).

292. The ‘right not to know’ is central to the assessment of the extent to which Art. 8(1) is engaged by the NDNAD system. Jorgen Husted argues that the imposition of unwarranted information (as in the Leicester example set out at section C-III above) is an autonomy issue, because choices and decisions must now be taken in the knowledge of information never previously requested, and thereby the individual loses the ability to direct his or her life as s/he might otherwise have wished (‘Autonomy and a Right not to Know,’ in Chadwick et al, *The Right to Know and the Right not to Know*, pp. 55 - 69).

293. It is suggested that in relation to whether Art. 8(1) is engaged, Baroness Hale alone was correct in the House of Lords. There is, undoubtedly, a *prima facie* interference with Art. 8(1) in this case.

294. The PACE regime challenged in both this case fails to recognise the five different aspects of privacy set out above. Classification of samples as ‘intimate’ and ‘non-intimate,’ and the resulting safeguards, consent requirements, and so on, are based purely on physical privacy grounds.

295. Art. 8(1) is engaged at two main stages in the forensic process: firstly, when the sample or fingerprint is taken; secondly, when each piece of material (sample, profile and fingerprint) are retained beyond the original purpose for which they were taken (samples and fingerprints) or generated (profiles).

296. As Art. 8(1) has presumptive weight, the acceptable limitations set out in Art. 8(2) must be strictly construed (*Sunday Times v UK*). In order to be justified, the interference must be in accordance with law, pursuant to a permitted aim and ‘necessary in a democratic society’. Each requirement is considered in turn below.

F. CONCLUSION

297. 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.

298. 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*.

299. 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.

300. 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, and the systems adopted by other Member States of the Council of Europe).

301. 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. 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 even have an independent custodian monitoring its use and access to the sensitive information it contains.

302. 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.

303. The presumption of innocence is an important, long-standing principle in the law of England and Wales, and the current retention regime under PACE undermines that principle. In addition, the PACE retention regime begins with the assumption that Art. 8(2) interests are to be broadly construed and have presumptive weight over Art. 8(1) rights, a reversal of the approach of the European Court of Human Rights. Rather, Art. 8(1) should have presumptive weight, with Art. 8(2) limitations to be strictly construed. 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.

I believe that the facts stated in this witness statement are true.

……..

Signed by Dr. Caoilfhionn Gallagher Date