COMMENTS IN RELATION TO THE QUESTIONS POSED BY THE ECHR IN THE CASE OF S. AND MARPER (APPLICATION 30562/04 & 30566/04) AND WHICH RELATE TO THE APPLICATION OF DATA PROTECTION LAW TO THE RETENTION OF DNA PERSONAL DATA

SUMMARY OF MAIN POINTS 2

FACTORS WHICH RELATES TO Q1 OF THE ANNEX 4
1. Does data about a DNA profile constitute personal data? 4
2. Reasons why DNA profiles differ from fingerprints? 5
3. Is the Article 8 right engaged? 7
4. How do the DPA and HRA interact? 8

FACTORS WHICH RELATES TO Q2 OF THE ANNEX 10
How do procedural safeguards Recommendation R(92)1 contrast with UK practice 10
Point 1: Retention of DNA personal data and DNA samples 10
Point 2: The deletion of DNA personal data is needed to implement recommendation 3 12
The precautionary principle 13
Point 3: Supervision of the DNA database 14

OTHER DATA PROTECTION ISSUES NOT MENTIONED TO R(92)1 15
A. Exaggeration and the impact on "purpose" of the processing 15
B. Unfair processing and Discrimination 17

MAIN CONCLUSIONS OF A DATA PROTECTION ANALYSIS 18
A database to span the population is inevitable 20

Dr. C.N.M. Pounder
E-mail: chris.pounder@amberhawk.com

March 2007

(**Note:** sent to Marper's legal team in March 2007 when I worked at PinsentMasons)

SUMMARY OF MAIN POINTS

(a) There needs to be a clearer delineation of the purpose behind the laws which can impact on privacy. On the one hand there are obligations which arise from national data protection law derived from the Council of Europe Convention No. 108 (which relates to the automated processing of personal data). On the other hand, there are obligations which derive from Article 8 of the Human Rights Convention. The Marper case before the Court allows this relationship between Article 8 and data protection to be defined.

(b) The functional difference between the two sets of obligations is determined by considering the main focus or purpose of the respective legal obligations. The main focus of the Article 8 obligations is to assess whether any interference by a public authority is lawful by reference to the tests posited by Article 8(2). The tests posited by Article 8(2) focus on **whether** personal data are lawfully processed.

(c) By contrast, the main focus of the data protection obligations is to provide a means of assessing the "proportionality" of any interference whenever personal data are processed. In this way, the data protection obligations sit underneath Article 8, and come into play when a determination of proportionality needs to be undertaken. This assessment of proportionality is by reference to a number of data protection principles which determine **how** personal data are processed (not **whether** personal data should be processed). For example, the processing of personal data in the context of issues such as retention, fairness, purpose limitation, relevance, security, accuracy, and rights of access to personal data.

(d) The consideration of **ALL** these data protection principles allows a rounded view of "proportionality" to be assessed. This leads to consideration of the Recommendations of the Council of Europe in the field of data protection, which although non-binding on Member States, provide a yardstick under which one can objectively consider data protection obligations and therefore "proportionality". These Recommendations are produced by a Committee of Experts drawn from Member States and carry the endorsement of the Council of Ministers.

(e) It follows that if there are a number of significant departures from its provisions of a Recommendation in the field of data protection, then this is a strong signal that the processing is

disproportionate in terms of Article 8. If there are very few departures from a Recommendation, then this is a strong signal that the processing is proportionate.

(f) In making an assessment of proportionality by reference to a Recommendation, it is irrelevant whether a Member State enters a derogation or not. This is because a Recommendation still defines best data protection practice even if it is non-binding on Member States, even though there is no requirement on a Member State to implement the Recommendation in legislation.

(g) The House of Lords analysis of the legal requirements is therefore incomplete because when it considered whether the processing of DNA personal data was proportionate, the Court:

I. did not consider the context of the requirements of the legislation derived from the Council of Europe Convention No 108 (i.e. the UK's Data Protection 1998).

II. did not consider the relevant recommendations of the Council of Europe in R(92)1 in the field of data protection and, in particular, the retention of DNA personal data.

III. overlooked the implications for familial DNA in that DNA personal data can now be related to more than one living individual and the potential for this development to interfere with the life of any member of Mr. Marper's family in a wider sense.

IV. failed to form a rounded view of how the data protection principles apply to the retention of DNA samples and DNA personal data.

(h) English law fails to distinguish between DNA and other samples (e.g. fingerprints) when the evidence suggests that DNA is unique, and that DNA personal data are in a unique position in need of additional protection

(i) The concept of proportionality in the context of DNA personal data should involve a precautionary principle test which can be applied in relation to the retention of DNA personal data to those who are arrested but not convicted of an offence. It is also argued that if the DNA of these people were necessary, then this could be achieved by an alternative route (e.g. recollection of the sample).

(j) It is likely that the DNA database will span the whole population, irrespective of the outcome of the Court's deliberations.

FACTORS WHICH RELATES TO Q1 OF THE ANNEX

1. Does data about a DNA profile constitute personal data?

It is taken as fact that the information comprising a digital representation of that DNA sample is automatically processed data (e.g. in a database) and that the only question to resolve is whether the data are also personal data as defined in data protection law. (This text uses the phrase "DNA personal data" to describe the digital representation of a DNA sample which can be related to a specific individual).

The definition of personal data under the Data Protection Act 1998 is:

> "**personal data**" means data which relate to a living individual who can be identified-
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

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

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

A DNA sample is widely believed to be unique for an individual, save for identical twins. Thus it can be assumed that the digital representation of that DNA pattern derived from a sample of DNA (e.g. found at the scene of crime) is also unique and is ***intended*** to relate to a specific individual. In the case of Marper, the police knew the data subject's identity, as this was established at arrest and around the time the sample was taken. Mr Marper was therefore "identified".

In the case of the DNA found at the scene of a crime which relates to an unknown individual, the police are very likely to want to establish the identity of the individual concerned, so that he or she – assuming that person to be a suspect - can arrested, by the police, at a later stage of the investigation. The intention is to identify the individual concerned.

The fact that the DNA database is linked to the Police National Computer provides evidence of linking the DNA digital representation to other name-linked personal data. The "DNA Good Practice Manual, Second Edition 2005" (published by the Association of Chief Police Officers (ACPO), states that DNA should not

be taken from an "Arrestee or Volunteer" if there is a marker on the PNC stating that a DNA profile is already held.[1]

Liberty[2] in its submission to the Nuffield Council on Bioethics Consultation: "Forensic use of bioinformation: ethical issues", January 2007, also confirm linkage of the DNA Database with other police systems. This states that the privacy implications of the DNA database "are exacerbated" by its connection to the Police National Computer because: "(a) connections can be drawn between sets of personal data: (b) PNC records are now retained indefinitely as a result of the link to the Database, whereas before they would have been weeded after a short period of time; and (c) information from the NDNAD, contained on the PNC, is visible to a wider range of non-policing bodies".

The fact that the digital representation of DNA might not be unique (i.e. it is mathematically possible, although unlikely, that more than one individual, could have a sufficiently similar digital representation of a DNA pattern even though they are not identical twins) does not detract from the **intent** of the police to identify a particular individual. This mathematical problem (if it exists) is more a reflection on the algorithm used to develop that digital representation. It can be anticipated that as such techniques refine or develop, this problem is likely to become more remote, and it therefore follows that any argument on these lines should carry little weight.

It follows that the digital representation of a DNA sample is personal data in terms of the Council of Europe's definition (Convention no. 108 provision). Additionally in Mr. Marper's case, the police will have other information in its possession which relates the digital representation in the DNA database to other information about Mr. Marper. **It follows that such data are also personal data and the data protection requirements of the Convention are engaged**.

2. Reasons why DNA profiles differ from fingerprints?

The prime reason why DNA is unique is that DNA contains information which relates to an individual's genetic history, and this has resulted in the development of techniques so that those related to that individual can be identified (e.g. via the use of statistical methods to identify familial relationships). It is expected that these techniques will develop and become more sophisticated. Additionally, DNA information about an individual also has the potential to reveal genetic predispositions or medical issues which the data subject might not be aware, or which will become apparent in later life, or which reveal

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

unknown relationships (e.g. paternity of children). All this genetically deduced information is not present in a mere fingerprint sample.

Liberty's[3] response to the Nuffield Council on Bioethics Consultation provides examples which illustrates why DNA and fingerprints differ. It notes that "familial searching could also unwittingly reveal to the police information about private personal relationships" as "A genetic link between individuals might be previously unknown to one or both parties and police investigations may make this information known for the first time. This is a serious concern given that it is estimated that around 1 in 30 people in the UK are mistaken as to the identity of their biological father. Familial searching also risks disclosure by police of the fact that an individual has been arrested to their family members".

This provides one important reason as to why DNA profiles differ from fingerprints and should be treated separately, a view supported by the Court in its provisional consideration of the Van der Velden application. Here the Court said[4]:

> "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".

Justice[5,] in its submission to the Nuffield Council on Bioethics is also convinced that fingerprints differ from DNA profiles. It states:

> "it seems clear that the analogy drawn between police retention of suspects' photographs and fingerprints – the basis of previous decisions of the European Commission of Human Rights in McVeigh, O'Neill and Evans v UK ((1985) 5 EHRR 71) and Kinnunen v Finland (App. No. 24950/94, 15 May 1996, unreported) - and police retention of DNA samples in Marper fails to compare like with like. Fingerprints contain no intrinsic bioinformation other than as biometric identifiers. While police retention of a suspect's fingerprints may constitute an interference with personal privacy, the interference in such cases seems minimal. The amount of medical information contained in an individual DNA sample, by contrast, seems to us difficult to understate. As the consultation paper itself notes, 'the analysis of DNA can reveal sensitive

---

2 Paragraph 17

3 Liberty's response to the Nuffield Council on Bioethics Consultation:"Forensic use of bioinformation: ethical issues", January 2007, Paragraph 19

4 Decision as to the Admissibility of Application 29514/05, Hendrick Jan Van der Velden against the Netherlands (section 2 of "The Law" analysis)

5 Forensic use of bioinformation: ethical issues, Nuffield Council on Bioethics, January 2007, paragraph 8

information about family relationships. Personal medical information may also be obtained by analysis of DNA samples'. We would go further and argue that the genetic information contained in DNA represents the most intimate medical data an individual may possess. The knowledge that an unspecified number of people may have access to that information over an indefinite period must surely constitute an interference with personal privacy. In the circumstances, a sensible analogy between police retention of fingerprints and police retention of individual DNA samples is difficult to sustain".

If the above analysis is correct, it follows that case law should place DNA in a unique position. However, despite these differences, Liberty[6] has provided an analysis which shows English law fails to distinguish between DNA profiles and fingerprints. Liberty makes the following comments:

(1) The Police and Criminal Evidence Act (PACE) makes no distinction in this context between fingerprints, samples, or the information derived from samples (See, for example, 63A(1), or 64(1A)) notwithstanding that the information that may be obtained from each (and therefore the "private" nature of each) may be very different.

(2) The uses that may be made of such fingerprints and samples are now not limited to checks made under section 63A (i.e. the "checking against other fingerprints and samples" (Section 63A(1)). They now merely "include" such checks (See section 64(1B)(a)-(c)).

(3) 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 three heads5:

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

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

(c) ***" the conduct of a prosecution"***.

The use under (b) appears to be the only category that has been referred to in this case thus far. However, Liberty is equally concerned with the potentially wider and more general scope of uses for the purposes ***"related to the prevention or detection of crime"***. On the face of it, this would include intelligence gathering and other forms of collation of detailed personal information, outside the immediate context of the investigation of a particular offence. (***Liberty's emphasis***).

3. Is the Article 8 right engaged?

The answer is yes, and Justice[7] summarises the position as follows:

"Secondly, recent case law from the European Court shows that retention by the police of personal information can plainly amount to an interference with the right to respect for personal privacy under Article 8(1). In Rotaru v Romania,(2000) 8 BHRC 43) for instance, the Court held that the collection, storage and use by a public authority of personal data interfered with the right to privacy under Article 8(1). In addition, in Peck v UK, [2003) 36 EHRR 41] the dissemination of

6 Third Party Intervention in the case of S and Marper v Chief Constable of South Yorkshire C/2002/0880 and C/2002/0081 (June 2002

7 Justice response Forensic use of bioinformation: ethical issues, Nuffield Council on Bioethics, para 9&10

> CCTV footage in a public street was held to interfere with the right to respect for privacy. Finally, in Friedl v Austria [1996) 21 EHRR 83],the Commission held that the retention of photographs of individuals identified by the police interfered with Article 8(1). Given the findings of interference with Article 8(1) in cases of photographs or CCTV, it seems deeply unlikely that the European Court of Human Rights would concur with the view of the House of Lords in Marper that the indefinite retention by the police of DNA information which contains personal and sensitive data does not also constitute an interference with the right to respect for privacy under Article 8(1) ECHR".

Justice's submission continues:

> "Thirdly, if we are correct that the Court would likely find that police retention of DNA samples would constitute an interference with Article 8(1), we further consider that it will find the retention of DNA samples of persons suspected, but not subsequently convicted, of an offence to breach Article 8(2) on the basis that such retention is unnecessary and disproportionate. Specifically, the principle of proportionality under human rights law requires that any interference with fundamental rights must be proportionate to the legitimate aim being pursued. In the case of police retention of bioinformation, therefore, it would require the legitimate interest of detecting and preventing crime to be balanced against the right of individuals not to have their personal information held without their consent. Furthermore, the principle of proportionality requires that the more intimate the data retained, the more important the competing interest has to be. Thus, while the legitimate interest in the prevention and detection of crime may justify the retention of DNA profiles of those proven guilty and charged, it cannot serve as a justification of the indefinite retention of DNA of individuals who are by law presumed to be innocent (Article 6(2) ECHR.7) A DNA database established in the interest of the investigation and prevention of crime may not be misused to gradually attain a comprehensive national database by including individuals who have not been proven guilty. In our view, the creation of a suspect database cannot be justified as necessary and proportionate under Article 8(2)".

In a footnote, Justice note "Similarly, the retention of information about a person's private life on a police register or by public authorities amounts to an interference with the right protected under Article 8(1); Leander v Sweden (1987) 9 EHRR 433, Hewitt and Harman v UK (1992) 14 EHRR 657".

4. How do the DPA and HRA interact?

The House of Lords did not consider any data protection obligations in its Marper judgement. Given the overlap between human rights and data protection, the case before the Court provides an opportunity for clarifying how these laws impact on private and family life.

The functional difference between the two is determined by considering the main purpose of the respective legal obligations. The main focus of the Article 8 obligations is to assess whether any interference by a public authority is lawful by reference to the tests posited by Article 8(2). The tests posited by Article 8(2) focus on whether personal data are lawfully processed. For example, the first part of the Article 8 establishes that "Everyone has the right to respect for his private and family life, his home and his correspondence" and Article 8(2) provides exceptions by stating that "There shall be no interference by a

public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

This means that any interference with the Article 8 right must pass three legal tests. Is the processing of personal data in accordance with law? Is the law pursuant to one or more of the interests of the legitimate objectives identified in Article 8(2)? Is the law "necessary in a democratic society?". Note that the these legal tests mainly apply to question "**whether** the processing should occur?".

By contrast, the main focus of the data protection obligations found in Council of Europe Convention No 108 is to provide a means of assessing the "proportionality" of any interference in those cases where personal data are processed. In this way, it can be seen that the data protection obligations sit underneath Article 8, and only come into play when a determination of the proportionality of the processing needs to be undertaken. This assessment takes place by reference to a number of data protection principles which relate to not **whether** personal data should be processed but rather **how** personal data are processed (e.g. the principles apply in the processing context in relation to issues such as retention, fairness, purpose limitation, relevance, security, accuracy, and rights of access to personal data). The consideration of ALL these data protection principles allows a rounded view of "proportionality" to be assessed.

This in turn leads to consideration of the Recommendations of the Council of Europe in the field of data protection, which although non-binding on Member States, provide a yardstick under which one can objectively consider data protection obligations and therefore "proportionality". These Recommendations are produced by a Committee of Experts drawn from Member States and carry the endorsement of the Council of Ministers apply the Convention's data protection principles to specific situations (e.g. policing, health, personnel).

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

FACTORS WHICH RELATES TO Q2 OF THE ANNEX

How do procedural safeguards Recommendation R(92)1 contrast with UK practice

The procedural safeguards are discussed by comparing UK practice in the context of R(92)1 which relates to the use of analysis of DNA in the framework of the criminal justice system. The Recommendation was adopted by the Council of Ministers in February 1992, and the UK Government has not, so far, derogated from its provisions.

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

The UK position appears to be that the retention of DNA personal data is always relevant to the policing purpose so it follows that the DNA personal data need not be deleted. By contrast R(92)1 takes a different view and the differences, which relate to retention, are summarized below.

Point 1: Retention of DNA personal data and DNA samples

1). R(92)1 recommends in paragraph 8, that "measures should be taken to ensure that the results of DNA analysis are deleted when it is no longer necessary to keep it for which it was used". This, to make sense, infers a retention period which is shorter than the life time of the data subject because otherwise this recommendation would be otiose. Paragraph 8 also recommends "strict storage periods" – another otiose provision if the UK position is intended by the Recommendation. In general, paragraph 8 infers that DNA personal data are deleted after some time-limit.

The usual practice in the UK, by contrast, is to retain DNA personal data indefinitely, including after the death of data subject, for a period which is not determined by a law . This is confirmed by the ACPO manual, DNA samples of Arrestees are NOT removed, even after the death of the original provider of the DNA sample[8] or from volunteers, if they give permission for the DNA

8 ACPO DNA Good Practice Manual, Second Edition 2005, paragraph 4.3

sample to be held on the database[9]. The police do permit samples to be deleted from the DNA database, but only if exceptional circumstances apply.[10]

2). R(92)1 also recommends, in paragraph 8, retention of DNA in cases of serious offences ("where the individual concerned has been convicted of a serious offence") or where the security of the state is involved. This recommendation also is otiose with respect to the UK practice of indefinite retention of DNA personal data in **all** circumstances (including after the death of data subject). The Recommendation also carries the implication that in cases where less serious offences have been proved to have been committed, DNA profiles and related DNA personal data should not be retained beyond a reasonable time which has been established by law. If this is the case, it follows that DNA data from those acquitted or not proceeded with should also be deleted after a reasonable time

This factor was also recognized in Van der Velden[11] where the "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. 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" (our emphasis).** This also implies that minor offences might not need to be associated with a DNA sample, and it follows that DNA for those not convicted following arrests should not be retained.

3). R(92)1 recommends in paragraph 8, that DNA personal data can be retained if the individual concerned "so requests". Any normal interpretation of this provision would include the prospect that individuals who provide samples can change their mind, and if they do so, the personal data related to the sample and the sample itself are deleted. In the UK, consent once it has been given cannot be revoked although the police tell individuals that consent cannot be revoked.[12] If R(92)1 wanted to adopt the UK position, it would have included the word "indefinitely" in its text.

A UK Parliamentary Committee has commented that it cannot understand the Government's position on consent.[13] It has stated that "We do not understand why consent should be irrevocable for individuals who are giving DNA samples on a voluntary basis". By contrast, the Government say for its part claims that (a) it would hinder the administration of justice if samples which should

9 ACPO DNA Good Practice Manual, Second Edition 2005, paragraph 4.4

10 Letter dated 31/1/2006 containing "Retention Guidelines – Exceptional cases" (for deletion of DNA) sent to all Chief Constables fro ACPO (Ian Readhead)

11 Decision as to the Admissibility of Application 29514/05, Hendrick Jan Van der Velden against the Netherlands (section 2 of "The Law" analysis

12 See reference 5

have been destroyed were in fact retained and then subsequently challenged; that (b) the withdrawal of consent is a precursor to criminal activity and that (c) it is administratively convenient[14] to keep the DNA data, as the law abiding person has nothing to fear. The Government told the Committee.

> "The rationale for not permitting a volunteer to withdraw their consent to their profile being retained on the national DNA Database is to avoid a return to the situation prior to the Criminal Justice Act 2001. Situations where consent had been given and then withdrawn, but for whatever reasons the profile remained on the database and was found to match that taken from a crime scene, could lead to arguments as to the admissibility of such evidence in any subsequent criminal proceedings. Withdrawal of consent could also be a precursor to future illegal activity. The information held on the database is only used if a stored sample is matched with a sample recovered from a crime scene. As with individuals acquitted of an offence for which DNA was taken and those whose prosecutions are not proceeded with, a law abiding person has nothing to fear from having their profile on the database."

Paragraph 8 of R(92)1 does not make reference to the above criteria as justifying retention if DNA personal data; by contrast it sets out "strict limits" on the retention of such data (see following).

4). R(92)1 recommends in paragraph 8, that "where the security of the state is involved, the domestic law of the member state may permit retention of samples …even though the individual concerned has not been charged or convicted of an offence". The Recommendation continues "In such cases, strict storage periods should be defined by domestic law.

The practice in the UK differs from the Recommendation as:

(1) the purpose of indefinite retention is not limited to state security

(2) no storage periods have been defined in domestic law, and

(3) DNA personal data are retained beyond the death of the individual concerned.

Point 2: The deletion of DNA personal data is needed to implement recommendation 3

R(92)1 recommends in paragraph 3, that DNA personal data **should** not be used for other (non-policing) purposes without Parliamentary approval. Restrictions on the retention of DNA personal data are essential safeguard for this obligation as if DNA personal data are retained, then the potential for wider use of DNA personal data is omnipresence. If however personal data are deleted, **they cannot possibly be used for other purposes**.

---

13 Paragraph 75 of Seventh Report of Session 2004-05, Forensic Science on Trial, Science and Technology Committee (Commons)

14 Government Reply to the Select Committee Report in reference 13

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

In the House of Lords in Marper[15] it was recognised (the Liberty argument) that if the DNA personal data were to be retained then other use would be possible. However, the Court determined that because the law prohibited wider use of the sample or data, and because the data did not reveal medical implications[16], and because the Court could revisit its decision if there were to be further use[17], then it followed that the Court could ignore the Liberty argument.

Even if there are statutory prohibitions on the wider use of DNA personal data, the retention of DNA personal data, is taking an unnecessary risk with the protection of the public; statutory barriers can easily be lifted. If it is deemed that DNA personal data are not needed by the police, then deletion ensures that there could be **no possible risk of further use of those data**.

The precautionary principle

In issues involving national security and public health, the Government often make use of the "precautionary principle" on the grounds that it is better to be safe than sorry. It is interesting to note that this principle has been applied, by Government, in the field of data protection, to protect special public interests. It follows that the same precautionary principle can be used to protect DNA personal data which after all, represents a special private interest which is unique to each individual.

For example, in relation to a disclosure of personal data to the Information Commissioner, the UK's data protection regulator, the precautionary principle was applied by Government when it refused permission for the Information Commissioner to inspect personal data, personally, in Government Offices. The Government claimed that as the personal data were subject to the national security exemption,[18] and the "precautionary principle" meant that was safer not to permit the Information Commissioner to inspect the personal data. In a letter to the Information (National Security) Tribunal, the national security interests explained that:

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

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

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

18SSHD, R(on the application of) v Information Tribunal & Information Commissioner [2006]EWHC 2958 (Admin)(23 Nov 2006)

> "26. Consequently the precautionary principles underlying the protection of national security required the respondent to regard the information as at risk of further disclosure to .... (or other members of the public) once it has been disclosed to the appellant" (the appellant in the case was the Information Commissioner, the UK's data protection regulator).

The same **precautionary principle** is implicit in paragraph 3 in the context of DNA personal data. It implements the requirement by removing the risks in the future which arise when DNA techniques evolve or because DNA can be related to more than one person. For example Liberty Report that [19]the UK's National Identity Register for the ID Card could be a natural linkage for a DNA database. The Daily Telegraph (5th November 2006) reported that this system "will have links with other Government systems to share identity data" and even suggests that the biometric data element of the NIR will, in fact, be stored on "existing biometric systems".

The precautionary principle does not interfere unduly with police practice should the need arise For example, the principle does not prevent them processing DNA personal data on arrest or making comparisons to see if the individual is connected with crimes committed in the past. The precautionary principle does not even require deletion of the DNA personal data immediately or in every case. To satisfy the precaution principle, given the special nature of DNA, requires a properly constructed retention schedule which specifies criteria which permit deletion to occur. As stated above, there is no such schedule in the UK except to say that DNA personal data are retained indefinitely.[20]

However, suppose in some future time there is a need to collect samples from those whose DNA sample has been deleted (for example, those arrested but not proceeded against). As the police have their identity of those they have arrested and have powers to access the tax, driver licence authorities or national identity systems to trace the individual concerned, they can easily fin the individual concerned. So, in cases such as Mr. Marper, retrospective collection of DNA and fingerprints, would be practicable.

Point 3: Supervision of the DNA database

R(92)1 recommends in paragraph 4, that DNA analysis should be carried out in circumstances determined by domestic law. However, as the Liberty analysis shows,[21] the law does not distinguish between fingerprints and DNA samples – even though they are different.

19 Liberty's response to the Nuffield Council Bioethics Consultation "Forensic use of bioinformation: ethical issues, paragraph 17, January 2007

20 ACPO DNA Good Practice Manual, Second Edition 2005, para tbc

21 Liberty's Third Party Intervention in the case of Marper before the House of Lords

However, Liberty's analysis make no mention of familial testing of DNA (when the DNA of one individual is related to another) although this issue was the subject if comments made by the Science and Technology Parliamentary Select Committee ("Forensic Science on Trial", session 2004-2005)[22] where it commented:

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

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

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

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

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

OTHER DATA PROTECTION ISSUES NOT MENTIONED TO R(92)1

A. Exaggeration and the impact on "purpose" of the processing

In one of its many submissions to the Home Office,[23] Liberty stated that "it was not aware of any evidence which supports the hypothesis that the detection of crime is improved by including DNA profiles from people who are arrested but not charged, or people against whom charges are dropped or are found to be innocent, as compared with retaining DNA profiles taken at random from the population". According to Liberty, this has been accepted by the Government on 9th October 2006, when Joan Ryan MP stated “As

22 See reference 14

23 Liberty's response to the Home Office Consultation "Standard Setting and Quality Regulation in Forensic Science, paragraph 7, November 2006

far as we are aware, there is no definitive data available on whether persons arrested but not proceeded against are more likely to offend than the population at large."[24]

Liberty added: "There is no basis for distinguishing these people from the population as a whole and the current approach therefore discriminates against them. In addition, there is no evidence that the detection of crime is improved by increasing the size of the Database. This is illustrated by the fact that, although there has been a massive extension of the NDNAD over the last 3 to 4 years, the rate of crime detection using the Database has stayed at about 0.35% of all recorded crime. If extending the size of the NDNAD had been successful one would expect this proportion to have increased".

Liberty continued: "We would also point out that the usefulness of the DNAD is driven by the ability to obtain DNA from the crime scene. In many cases DNA is not available. Furthermore, the identity of the suspect is not in question and in a high proportion of cases and, in these, the ability to match crime-scene DNA would not facilitate prosecution".

If these claims for exaggeration are correct, they will engage with many data protection issues via the "purpose" of the processing of personal data. If exaggerated claims are proven, then this reduces the justification for the purpose of the processing in the first place. To illustrate the data protection point, it is useful consider most of the Quality Principles in Article 5 of Convention No 108.

Article 5 states under the heading "Quality of data":

> Personal data undergoing automatic processing shall be:
>
> obtained and processed fairly and lawfully;
>
> stored for specified and legitimate purposes and not used in a way incompatible with those **purposes**;
>
> adequate, relevant and not excessive in relation to the **purposes** for which they are stored;
>
> accurate and, where necessary, kept up to date;
>
> preserved in a form which permits identification of the data subjects for no longer than is required for the **purpose** for which those data are stored" (our emphasis on **purpose**)

Note that these Principles gain their meaning by reference to the purpose of the processing, then any wide and unjustified claim for the purpose of the processing, undermines these principles. It is noted that these worries could not exist if a **precautionary principle** was in place.

24 8th October 2006, HC Deb, col 491W

B. Unfair processing and Discrimination

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

In the UK, in case of MDU v Johnson[25], the concept of fair processing arose in a case where it was argued that the outcome of the processing of personal data caused an individual particular detriment. The case involved the use of a risk assessment system by an insurer, the use of which resulted in a health professional having his medical insurance cover withdrawn. The health professional sued for damages and argued that the outcome of the processing was unfair because he had been subject to a faulty risk assessment procedure. The Court's judgment was that the processing was fair because the risk assessment procedure had been applied to everyone who had applied for insurance.

The Court commented in this case:

> "123. It is easy to see how he regards the decision in his case as unfair but it has to be remembered that the policy is directed at risk management – at preserving the MDU funds against a risk of claims, and the incurring of costs, in the future…..The MDU is entitled first to determine its policy. Having done so, it then has to ensure that any processing of members' data in line with that policy is carried out fairly".

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

For example, Liberty[26] states that it is "profoundly concerned" about the disproportionate number of black men on the NDNAD. 37% of black men have their DNA on the database. Within the Metropolitan Police area, 51% of the innocent (uncharged) people whose DNA is held on the Database are of black or BME origin. This disproportionate representation of black men on the Database exacerbates and reinforces discriminatory police practices which are well-documented.

Action on Rights for Children , in its submission to the Nuffield Council consideration of "The Forensic Use of Bioinformation: Ethical Issues" stated that "Arrests and disposals: 10-17-year-olds 2005" that the provisional figures indicate that 348,000 (or 24%) of all arrests in 2005 were of 10-17s.[27]. They state that

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

26 See reference 20

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

118,900 10-17s received reprimands (69%) or final warnings (31%)[28] and 96,300 were convicted in the courts [29]. This means that "Thus in total there were 215,200 disposals, and 132,800 arrests did not lead to any disposal". ARC adds "The 2004 figures are remarkably similar to the 2005 figures above, when 330,800 arrests led to 195,500 disposals. 135,300 arrests did not lead to disposal".

Assuming all arrests, as in the case of Marper, lead to a DNA profile being taken this means that in over one-third of 10-17 disposals where no prosecution follows, a profile is taken. With familial techniques developing, the taking of DNA of a young person will map that person's family as well. This in turn leads to the question of whether the processing of personal data in these circumstances is fair.

For example, if the DNA database spanned nearly 100% of a particular minority grouping based on race, is there a risk that the police could target members of that community on the grounds that gradually, with familial testing taken into account, the possession of DNA personal data will span the whole of that community and ease detection of crime within that community. If so, would this be "unfair processing"?

The point being raised here is that this case can be argued (following MDU v Johnson) if DNA is retained disproportionately amongst certain members of the society, with the result that this community is targeted by the police. It is noted that these worries could not exist if a **precautionary principle** was in place.

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

MAIN CONCLUSIONS OF A DATA PROTECTION ANALYSIS

Data protection law would not preclude the taking of a DNA sample from somebody arrested and using information derived from that sample in relation to an inquiry. A data protection law would not prevent DNA personal data derived from a sample being processed and comparisons been made with samples

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

found at the scene of a crime or other scenes of crime. A data protection law would not require DNA personal data to be deleted by the police, if such data could be justified in terms of their current inquiries.

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

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

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

(a) those identified individuals who are convicted of minor offences.
(b) those identified individuals who are convicted of serious offences.
(c) Juveniles who are processed by the criminal justice system
(d) those identified individuals who are arrested and whose DNA matches that found at another scene of crime.
(e) those identified individuals who are arrested but are not convicted or proceeded against.
(f) those identified individuals whose samples need to be eliminated from the DNA found at the scene of crime.
(g) those unidentified individuals whose DNA is found at the scene of a crime.
(h) those who consent to the DNA personal data being processed.

Sometimes there can be overlap. For example, DNA personal data in category (b) and (g) are likely to be kept indefinitely whereas (h) would be retained until consent is withdrawn; some special rules might apply for category (c) and the retention times for (a) would be longer that (e). However, this **approach appears**

29 Ibid (Table 3.7)

30 http://www.homeoffice.gov.uk/rds/pdfs/hosb401.pdf

not to be consistent with the UK approach of "one size fits all" and where all DNA personal data in the above categories are kept indefinitely.

A database to span the population is inevitable

The UK has a population of 60,000,000. Suppose there are very high statistically significant links of one profile to say 4-6 close members of a family (e.g. parents, brothers, sisters), then a database the current size of the DNA database 3.5-4 million entries can be expected to span about 20%-40% of the population. A database of 10,000,000 clearly has the potential span the whole population. As scientific techniques improve, it is to expected that the statistical techniques in relation to familial line DNA analysis can be extended to the more remote family members. The reason why the police keep DNA samples beyond the death of the person from whom the sample was taken is, in part, a tacit recognition that the DNA sample can relate to other individuals and that such techniques could improve familial tracing[31].

Criminal statistics regularly show that, approximately, about one third of males and one-tenth of women have a criminal record other than motoring offences[32]. Assume these level remain constant, and assume that DNA continues to taken from those convicted, the maximum DNA database coverage of the population will inevitably approach 25% (assuming DNA is taken from those men and women who commit a criminal records). The Court has already accepted in the case of Van der Velden[33], that because of his offences, his Article 8 rights were not infringed by the retention of DNA personal data and that there was no need to assess the data protection implications.

If also familial search techniques improve their accuracy (which is inevitable) and if we only assume that one DNA sample can be related statistically to 4 individuals (e.g. parents, one brother and sister), then it appears that most of the population will somehow relate to the DNA database which approaches 25% coverage. It is for this reason, the Court should take the opportunity of requiring selective retention criteria which can apply to minor offences as well as those arrested but not proceeded with.

In conclusion, a national DNA database of the future is likely to span 80%-100% of the population – the only question is when this will occur. If DNA personal data is limited by the Court (e.g. to those who possess a criminal record or who are arrested), then this will encourage the emergence of other techniques whose objective is to span those genetically related to the criminal. If the Court decides that indefinite

31 ACPO DNA Good Practice Manual, Second Edition 2005,Appendix 1)

32 See Hansard, 18 Apr 2006 : Column 287W or http://www.homeoffice.gov.uk/rds/pdfs/hosb401.pdf

33 See reference 4

retention of DNA personal data does not interfere with private and family life or data protection law, then the question is "why not require DNA samples of all citizens to be given to the police". And if this is the conclusion, why is the information given to the police limited to DNA?

Dr. Chris Pounder
chris.pounder@amberhawk.com
March 2007