AADHAR
VIOLATION OF PRIVACY

SITARAMAIAH CHALLA
Senior Advocate

ASIA LAW HOUSE
Hyderabad

Unless we make the requirement for administrative action strait and demanding, expertise, the strength of modern Government can become a monster which rules with no practical limits on its discretion. Absolute discretion, like corruption marks the beginning of the end of 'liberty' (96 Led 662)

The Nation and People shall not forget Justice Douglas warning.

I. RIGH TO PRIVACY:

The right to privacy is not enumerated as a fundamental right in the Constitution. It is implicit in the right to life and liberty guaranteed to citizens of the Country by Art.21. Art.21 has an exalted status in our Constitution, for even during emergency the right under Articles 20 and 21 cannot be suspended. It is a right to be left alone. A citizen has a right to safeguard the privacy of his own, his family and marriage.

A right to privacy can be physical characteristics, bodily substances and ones mental process. This is the guarantee of substantive due process, which is part and parcel of idea of personal liberty protected under our constitution.

---

see Karaksingh v State of UP 1963 SC 1295.

R Rajgopal v State of TN 1994(6) SCC 642,
Peoples Union of Civil liberties v UOI 1997(1) SCC 301

Substantive due process is the idea that some laws invade liberty or property in such a fashion, they cannot be considered as valid law.

II. INTERNATIONAL COVENANTS:

India is a party to the International covenant on civil and political rights and the international covenant on Economic, Social and Cultural Rights adopted by the General Assembly of the United National on 16th December, 1966. The human rights embodied in the aforesaid covenants stand protected by the Constitution. That is the reason the Nation passed an Act called "The Protection of Human Rights Act" in 1993. Sec 2(d) defines Human Rights means the right relating to life liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in International Covenants and enforceable by Courts in India. Section 2(f) states that International Covenants means "the international covenants on Civil and Political Rights and international covenants on Economic, Social and Cultural Rights adopted by the General Assembly of the United Nations on 16th December, 1966 and such other covenants or conventions adopted by the General Assembly of the United Nations as the Central Government may by notification specify

Article 17 of the International Covenants on Civil and Political Rights 1966 says

"17(1) No one shall be subjected to or unlawful interference with his privacy, family home or correspondence, nor to unlawful attacks his honour and reputation.

(2) Everyone has the right to the protection of the Law against such interference or attack.

Article 8 of the European Convention on Human Rights States: **ARTICLE 8:**

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. 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.

Art. 12 of the Universal Declaration of Human Rights (1948) refer to privacy and it states “No one shall be subject to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the Law against such interference or attacks.

Douglas Justice said “that privacy is a fundamental personal right, emanating from the totality of the Constitutional scheme under which we (Americans) live” Crisval v State of Connecticut (381 US 479 at 494) Justice Stevens in Thornburgh v American college of OIG

(476 US 787) said the concept of privacy embodies the moral fact that a person belongs to himself and not to others nor to the society as whole" (Justice R C Lahoti dealt all this elaborately in 2005(1) SCC 496 (District Registrar & Collector v Canara Bank).

III. The Right to privacy both on physical and mental sense in relation to involuntary administration of certain scientific techniques namely Narco analysis, Polygraph examination and Brain electronic activation profile (BEA) (proje) for purses of improving investigation efforts in criminal cases would this violate Art 21 Human Rights the privacy. In Selvi v State of Karnataka Balakrishanan CJ said

"244. It is undeniable that during a narcoanalysis interview, the test subject does lose "awareness of place and passing of time" It is also quite evident that all the three impugned techniques can be described as methods of interrogation which impair the test subject's "capacity of decision or judgment". Going by the language of these principles, we hold that the compulsory administration of impugned techniques constitutes "cruel, remembered that the law disapproves of involuntary testimony, irrespective of the nature and degree of coercion, threats, fraud or inducement used to elicit the same. The popular perceptions of terms such as "torture" and "cruel, inhuman or degrading treatment" are associated with gory images of blood-letting and broken bones. However, we must recognize that a forcible intrusion into a

person's mental processes is also an affront to human dignity and liberty, often with grave and long lasting consequences.) A similar conclusion has been made in the following paper; Marcy Strauss, "Criminal Defence in the age of Terrorism- Torture"

"262: In our considered opinion, the compulsory administration of the impugned techniques violates the "right against self incrimination". This is because the underlying rationale of the said right is to ensure the reliability as well as voluntariness of statements that are admitted as evidence. This court has recognized that the protective scope of9 Article 20(3) extends to the investigative stage in criminal cases and when read with section 161(2) of the Code of Criminal Procedure, 1973 it protects accused persons, suspects as well as witnesses who are examined during an investigation. The test results cannot be admitted in evidence if they have been obtained through the use of compulsion. Article 20(3) protects an individual's choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inclupatory or exculpatory. Article 20(3) aims to prevent the forcible "conveyance of personal knowledge that is relevant to the facts in issue". The results obtained from each of the impugned tests bear a "testimonial" character and they cannot be categorized as material evidence.

"263: We are also of the view that forcing an individual to undergo any of the impugned techniques violates the standard of

"substantive due process" which is required for restraining personal liberty. Such a violation will occur irrespective of whether these techniques are forcibly administered during the course o fan investigation or for any other purpose since the test results could also expose a person to adverse consequences of a non penal nature. The impugned techniques cannot be read into the statutory provisions which enable medical examination during investigation in criminal cases i.e., the Explanation to section 53, 53-A and 54 of the Code of Criminal Procedure, 1973. Such an expansive interpretation is not feasible in light of the rule of "ejusdem generis" and the considerations which govern the interpretation of statutes in relation to scientific advancements. We have also elaborated how the compulsory administration of any of these techniques is an unjustified intrusion into the mental privacy of an individual. It would also amount to "cruel, inhuman or degrading treatment" with regard to the language of evolving international human rights norms. Furthermore, placing reliance on the results gathered from these techniques comes into conflict with the "right to fair trial" invocation of compelling interest cannot Justify the dilution of constitutional "rights such as the right to self incrimination"[1]

1. SELVI v STATE OF KARNATAK 2010 (7) SCC 263.

IV. BIO METRICS & DNA

We are concerned with ‘Biometrics’ and DNA of an individual.

‘Biometrics’ means the technologies that measure and analyze human body characteristics, such as fingerprints, eye retina and irises, voice patterns, facial patterns hand measurements and DNA for authentication purposes. (Rule 2(b) of Information Technology information rules)

DNA stands for deoxyribonucleic acid, it is a chemical found in virtually every cell in the body and the genetic information therein. Which is the form of code or language, determines physical characteristics and directions the chemical process in the body.

Taking of the finger prints or taking of impression of the parts of the body could be only with permission of the Court when a person is accused of a crime and during the course of investigation (73 of Indian Evidence Act)

IDENTIFCATIN OF PRISONER’S Act.

Specifically provides that if a magistrate is satisfied for the purpose of any investigation or proceeding under the code of Criminal procedure 1898 that it is expedient to direct any person to allow his measurements or photograph to be taken he may make an order to that effect and no order shall be made unless the persons has some time been

arrested in connection with such investigation or proceedings. Section 7 of the said Act states that if the person is acquitted, discharged or released without trial the fingerprints photographs etc must be destroyed – unless the court other directs.

The finger prints cannot be taken in anticipation that he might commit a crime nor for the investigating authority to compare.

The Supreme Court of India in State of MP v Rambabu Misra emphatically held that the section 73 does not permit a Court to give a direction to the accused to give specimen writings for anticipated necessity for comparison in a proceeding what may later be instituted in the Court either in Civil or Criminal proceedings 1980(2) SC 343. Same view was held in American Supreme Court also Joe Hayes “Florida 470 US 811= 84 led (2) 705.

Prevention of Terrorism Act 2002 gives the power to the police officer investigating a case to request the Court for obtaining the samples, the section 27 read as follows:-

“27. Power to direct for samples etc. – (1) When a police officer investigating a case requests the Court of a Chief Judicial Magistrate or the Court of a Chief Metropolitan Magistrate in writing for obtaining samples of handwriting, finger-prints, foot-prints, photographs, blood, saliva, semen, commission of an offence under this Act, it shall be lawful for the Court of a Chief Judicial Magistrate or the Court of a Chief

Metropolitan Magistrate to direct that such samples be given by the accused person to the police officer either through a medical practitioner or otherwise, as the case may be.

(2) if any accused person refuses to give samples as provided in sub section (1), the Court shall draw adverse inference against the accused.

Section 5 of the Identification of prisoners Act states:-

5. Power of Magistrate to order a person to be measured or photographed:- If a Magistrate is satisfied that, for the purposes of any investigation or proceeding under the Code of Criminal Procedure, 1898, it is expedient to direct any person to allow his measurements or photograph to be taken, he may make an order to that effect, and in that case the person to whom the order relates shall be produced or shall attend at the time and place specified in the order and shall allow his measurements or photograph to be taken, as the case may be, by a police officer.

Provided that no order shall be made directing any person to be photographed except by a Magistrate of the first class:

Provided further, that no order shall be made under this section unless the person has at some time been arrested in connection with such investigation or proceeding.

DNA collecting samples can violate privacy:

"75. In the response of the Privacy Commissioner of Canada to Department of Justice Consultation Paper – Obtaining and Banking DNA Forensic Evidence, it is stated:-

"3. Collecting DNA from suspects – DNA evidence should not be collected from a suspect unless the information is relevant to a specific crime in question. For example, it would be appropriate to obtain a DNA sample from a suspect where DNA evidence is left at the scene of the crime and the suspect's DNA is needed to prove the suspect's involvement.

DNA evidence should not be collected from suspects as a matter of routine. To do so would cause an unnecessary privacy intrusion; in the vast majority of criminal cases DNA evidence will contribute nothing to the investigation. Thus, it would not be appropriate for Parliament to give blanket authority to collect DNA samples from all persons suspected of indictable offences. DNA should also not be collected from a suspect if investigators have no DNA evidence with which to compare the suspect's sample.

Nor would a DNA sample from the suspect be necessary if the suspect admitted guilt.

However, as a practical matter, the DNA evidence might be critically important in getting the suspect to admit guilt in the first place.

"As well, there should be reasonable grounds, for suspecting that the person committed the offence before taking the DNA sample. It would not be acceptable to require all men in a given community to submit DNA samples to solve a specific crime.

"Broad-based testing of whole groups within a community would represent an unjustifiable intrusion into the lives of too many innocent people. As a further privacy safeguard, DNA evidence should be collected from a suspect only if a judge authorizes the collection.

"In our 1992 Report, Genetic Testing and Privacy, we discussed limiting the collection of DNA samples to cases involving criminal violence. The types of violent crimes for which DNA samples might be collected should be set out in legislation. The list of violent crimes set out in New Zealand's recently introduced Criminal Investigations (Blood Samples) Bill officers and example of the types of crimes for which DNA testing might be considered in Canada. It may also be appropriate to allow the collection of samples for other crimes, such a conspiracies to commit offences involving violence. For example, it should be lawful for samples to be taken if DNA evidence could help convict someone suspected of planning a terrorist act or murder (perhaps the suspect had left DNA on a stamp he licked and attached to a letter implicated in the crime)"[1]

1. 2003(4) SCC 493 SHARDAV DHARM PAL

Rules were framed under Information Technology Act, 2000
(Act 21 of 2000)

Rule 2(b) defines Biometrics. It is quoted earlier rule 3 defines sensitive personal date or information. Rule 3(vi) states Biometrics information. Body corporate is defined that is the body corporate as defined in clause (1) of explanation to section 43A of the Act.

"Section 43A reads as follows:-43A. Compensation for failure to protect data:- Where a body corporate, possessing, dealing or handing any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation: - For the purposes of this section-

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, discloser or impairment, as may be specified in an agreement between the parties or as may be specified in any law

for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;"

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.]

This is a protective provision with the sole object to protect personal data and privacy.

Biometric information is classified a sensitive personal data information. Without the consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding the purpose of usage before Collector of such information. Rule 5(4) states that the body corporate shall not retain the information for longer than required for the purpose for which the information for the purpose the information may lawfully be used or otherwise required under any other law for the time being in force.

It is appositive assertion under the statute and an assurance to an Indian citizen that finger prints eye retina and irises, voice patterns, hand measurements and DNA shall not be collected without the

consent of the individual. The Supreme Court of India dealt with the right and held that it could be collected only when a person is accused and brought before a Court and with the permission of the court. All the Acts mentioned above specifically deals with the right of an individual. (The rules attached as an annexure to this article.)

V. CITIZENSHIP ACT 1955

Section 14A of the said Act states "Issue of National identity cards – The Central Government may compulsorily register every citizen and issue national identity card to him.

(2) The Central Government may maintain a National Register of Indian citizen and for that purpose establish a National Register Authority.

By virtue of power conferred under section 18(1) & (3) of the Citizenship Act, 1955 rules are framed under the said Act called the Citizenship (Registration of citizens and issue of National Identity cards) Rules in 2003. National identity card is issued to every citizen of India. Rule 13 states:-

13 Issue of National Identity Cards: - The Registrar – General of Citizen Registration or any officer authorised by him in this behalf, shall issue the National Identity Card to every citizen whose particulars are entered in the National Register of Indian Citizens under sub rule (3) of Rule 3.

14 National Identity Card to be Government property and responsibility of citizens to keep them properly: -

(1) The National Identity Card shall be the property of the Central Government.

(2) No personal shall willfully destroy, alter, transfer or use in any form the National Identity Card, except for the lawful purposes.

(3) On the happening of any of the events specified under sub rule (1) of Rule 10, the National Identity Card shall be surrendered by the citizen or his nearest relative, as the case may be, to the Registrar – General of Citizen Registration or any other authorised officer acting on his behalf.

(4) In the event of a loss of the National Identity Card, it shall be the duty of the citizen or his nearest relative, as the case may be, to report the matter immediately to the nearest police station and the concerned authority.

The National Identity card contain the particulars in rule 3 states.

3. National Register of Indian Citizens – (1) The Registrar – General of Citizen Registration shall establish and maintain the National Register of Indian Citizens.

(2) The National Register of Indian Citizens shall be divided into sub parts consisting of the State Register of Indian Citizens, the District Register of Indian Citizens, the Sub District Register of Indian Citizens and the Local Register of Indian Citizens and shall contain such details as

the Central Government may, by order, in consultation with the Registrar General of Citizen Registration, specify

(3) The National Register of Indian Citizens shall contain the following particulars in respect of every Citizen, namely –

(i) Name

(ii) Father’s name;

(iii) Mother’s name;

(iv) Sex;

(v) Date of birth;

(vi) Place of birth;

(vii) Residential address (present and permanent)

(viii) Marital status – if ever married, name of the spouse;

(ix) Visible identification mark;

(x) Date of registration of Citizen;

(xi) Serial number of registration; and

(xii) National Identify Number.

(4) The Central Government may, by an order issued in this regard, decide a date by which the Population Register shall be prepared by collecting information relating to all persons who are usually residing within the jurisdiction of Local Registrar.

(5) The Local Register of Indian Citizens shall contain details of persons after due verification made from the Population Register.

4. Preparation of National Register of Indian citizens:- (1) The Central Government shall, for the purpose of National Register of Indian Citizens, cause to carry throughout the country a house to house enumeration for collection of specified particulars relating to each family and individual, residing in a local area including the citizenship status.

(2) The Registrar – General of Citizen Registration shall notify the period and duration of the enumeration in the Official Gazette.

(3) For the purposes of preparation and inclusion in the Local Register of Indian Citizens, the particulars collected of every family and individual in the Population Register shall be verified and scrutinized by the Local Registrar, who may be assisted by one or more persons as specified by the Registrar – General of Citizen Registration.

(4) During the verification process, particulars of such individuals, whose citizenship is doubtful, shall be entered by the Local Registrar with appropriate remarks in the Population Register for further enquiry and in case of doubtful citizenship.

It is obligatory for every individual to get himself registered with the local Registrar of Citizen registration. This National Register of Indian citizen is maintained and is being updated.

National Identity card issued by the Election Commission of India carries the National Identity number allotted to every citizen by the Registrar general of citizens Registration (like J K 6097166) father

name, date of birth, thumb mark date of issue place of issue. It carries the assurance. The card may be used as an identity card under different government schemes”

In 2010 a bill called National Identification Authority of India Act 2010 was drafted and was introduced in Rajya Sabha (Bill LXXV of 2010).

It empowers the Central Government to establish an Authority known as National Identification Authority of India to exercise the powers conferred on it and to perform functions assigned to it even before the bill became law on 2nd July 2009. The Government appointed chairperson as Unique Identification Authority of India.

Section 3 states that every resident shall be entitled to obtain an aadhaar number on providing of his demographic information and biometric information to the authority in such manner as may be specified.

Demo graphic information includes information relating to the name, age, gender and address of an individual (other than race religion caste, tribe, ethnicity language income, health. biometric information means a set of such biological attributes of an individual as may be specified.

The bill lapsed.

In 2016 the Aadhaar (targeted delivery of Financial and other subsides, benefits and services) Act, 2016 was passed. It states that this is an Act to provide for, as a good governance, efficient, transparent and targeted delivery of subsides, benefits and services, the expenditure for which is uncured from the consolidated fund of India to individuals residing in India through assigning of Unique Identity number to such individuals and for matters connected therewith or incidental thereto.

The Act defines “Biometric information” a photograph, finger print, irises or other such biological attributes of an individual as may be specified by regulations. It defines demographic information. It includes information relating to the name, age date of birth and adverse and other relevant information of an individual.

Section 7 states proof of Aadhaar number necessary for receipt of certain subsides, benefits and services etc.,

7. Proof of Aadhaar number necessary for receipt of certain subsides, benefits and services, etc:- The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt there from forms part of, the consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number

or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment;

Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

This Aadhaar number, the act says is not evidence of citizenship or domicile section 9.

9. Aadhaar number not evidence of citizenship or domicile, etc:- The Aadhaar number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder.

When National Identity card is issued to every citizen of this Nation why does the Government insist on an individual to obtain Aadhaar card, with biometrics. The right of privacy is totally destroyed. This insistence is contrary to the decisions of the Supreme Court, Evidence Act and other Acts quoted earlier.

The World cannot forget human rights violations occurred during the Second World War. After the War Europeans from all walks of life gathered at the Hogue conference in response to the call issued by the council of Europe.

A hundred parliamentarians from twelve member states of the council of Europe gathered in Strasbourg in 1949 to draft a charter of Human Rights and to establish a Court to enforce it. The convention was opened for signature on 4th November, 1950 in Rome. It was ratified and came into force on 3rd September, 1953. It is overseen and enforced by the European court of Human Rights in Strasbourg [1].

Article 8 provides for a right to respect one's private life and family life, his home his correspondence.

It was pointed out in the beginning itself that India is a party to the International covenant on Civil and political Rights and the International covenant of economic social and cultural Rights. Section 17 also was quoted earlier. This Nation respects and follows the ideals embodied in the said international convention. Laws framed shall not violate these ideals. We respect them.

It is not necessary to go back to the questions raised during the World Wars I and II, regarding the identity cards, and the schemes.

---

1. From Wikipedia, the free encyclopedia and the citations at the end of the article and the references.

It is sufficient to quote the remarks by the historian AJP Taylor in his English history 1914- 1945.when he describes the whole thing an ‘indignity’ and talks of the Home guard harassing people for their cards. The conservative and liberal peers voiced their anger over what they called as ‘social’ card indexing. In 1951 the conservative administration was pledged to get rid of the scheme ‘to set the people free’.

In 1998 Data protection Act was enacted to implement the Data Protection Directive, the purpose of which is to harmonies data protection legislation throughout European Union in order to protect the fundamental rights and freedoms of the individual in particular the right to privacy with respect to the processing of personal data and to facilitate the free flow of personal data within the European Union. Data protection Act 1998replaced the Data protection Act 1984 and the access to personal Files Act 1987. The Data protection Act established a system of data protection controls for manual data as well as computerized data and adds extra safeguards where personal data was considered sensitive and establishes certain rights of the data subject.

Separate provision is made for processing of personal data and the protection of privacy in electronic communication sector and 2) with regard to control of patent information.

In 2006, the British Parliament passed an Act called Identity Card Act 2006, an Act to make provision for national scheme of

registration of individuals and for issue of cards capable of being used for indentifying registered individuals.

Section 5 mentions about applications relating to entries in Register sub section (5) of section 5 …(b) to allow his finger prints and other biometric information about himself, to be taken and record (5)(c) to allow himself to be photographed.

The conservative/liberal democratic coalition formed after 2010 general elections announced that I.D card scheme would be scrapped. The Identity card Act was repealed by the Identity documents Act 2010 on 21 January,2011, and the cards were invalidated with no refunds to purchasers. The repeal made all identity cards invalid and mandated destruction of all data on the National Identity register. It was said that this marks the final end of identity card scheme dead, buried and crushed.

In a document published in May 2010; the new Government announced that scrapping of the scheme would save approximately 86 million pounds following 4 years and avoids 800 million pounds in maintenance over the decades which were to have been recovered through fees. (I wonder what this Nation, India has spent for the Aadhaar card scheme and what it is going to cost for the maintenance). The Act provides “requiring Aadhaar numbers for indentifying an individual for delivery of benefits subsides and services,

the expenditure is incurred from or the receipt there from forms apart of consolidated fund of India”

UNITED KINGDOM (U.K)

In 2001 January police arrested one S arrested on charge of an offence of attempted robbery. Finger prints and samples were taken from him. Following a trial S was acquitted of the charge. Police refused to destroy the finger prints and samples stating that Criminal justice & Police Act 2001 gives the police the power, the right to retain finger prints and samples to aid crime and investigation, and the finger prints and samples will be retained. S sought judicial review of the decision to quash the policy to retain fingerprints and samples.

In March, 2001 Mr. Marper was arrested and charged with harassment by his partner Police took his finger prints and samples. He and his partner reconciled and the proceedings were dropped. Then Marker demanded destruction of his finger prints and samples. The police refused to destroy. When he moved the Court. The Court held retention of finger prints and the DNA samples of individuals who had not been convicted of a criminal’s offence did not contravene either individual right or right to private life.

Both the matters reached the House of Lord’s Learned Lord’s sat to decide the case. The majority dismissed the appeals. Bareness Hale of Richmond dissented’

Lord Steyn' said

Section 64(1A) of the Police and Criminal Evidence Act 1984 was substituted S.82 of 2001 Act, It provides

"Where (a) fingerprints or samples are taken from a person in connection with the investigation of an offence, and (b) sub section (3) below does not require them to be destroyed, the fingerprints or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution' (My emphasis)"

The Learned Lord states that the simple question before the House concerns the compatibility of 64(1A) with the European convention for the protection of Human Rights Act 1998 and in particular with the convention rights contained in articles 8 & 14.

The Learned Lord held "the policy to retain, save in exceptional cases all finger prints and DNA samples taken from those who had been acquitted of criminal offences or against whom proceedings have not been pursued was Lawful".

Baroness Hale dissented. It is stated

"(67) My Lords, sadly, while I agree with everything else in the opinion of my noble and learned friend, Lord Steyn, I cannot agree with the view, to which he is inclined, that the retention and storage of fingerprints,

1. 2004(4) All ER 193

DNA profiles and samples is not an interference with the appellant's rights under Art.8 (1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (as set out in Sch. 1 to the Human Rights Act1998).

"(68) I agree that it is necessary to distinguish between the taking of fingerprints and samples, the deriving of information from those samples, the storage of samples and information, and the use of either samples or information for some particular purpose. The justifications for each of these may be very different. But all of them, in my view, constitute an interference by the state in a person's right to respect for his private life. This is an aspect of what has been called informational privacy.

"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 (See R v Dyment (1998) 45 CCC (3d) 244 at 255 – 256 per La Forest J)

"(72) Hence it is common ground that the taking of fingerprints and DNA samples is an interference with the art 8(1) right, even though the invasion of bodily integrity involved is minimal. It is also common ground that the use of the information derived from them is such an interference. This must be because the information is regarded as intrinsically private.

"(73) If the taking and use of the information is an interference, it is difficult to see why the retention, storage or keeping of that information is not also an interference. Storing information almost inevitably involves someone else knowing it. It is an interference with privacy for someone to know or have access to private information even if they make no other use of it. The mere fact someone has read my private correspondence or seen my bank accounts is an interference with my privacy even if that person tells no one else what he has seen. That is why access to private information such as that contained in medial records has to be carefully controlled. The fact that only a few people can understand the information does not affect the principle, although it may affect the justification.

The emphatic statement was

"(76) The general tenor of the jurisprudence of the European Court of Human Rights (the Court of Human Rights) and European Commission of Human Rights (the Commission) is that the retention, keeping or storage of private information by state institutions is an interference with art 8(1) rights.

S and Marper carried the matter to the European Court of Human Rights[1]. The matter was referred a Bench of 17 Judge's in view of the importance of the subject and in view of the Judgment in Vander Velden v Netherlands. Decision in 29514/05 ECHR 2006.

1. DCHR application No.30562/2—4 & 3056604 European Court of Human Rights is of 47 countries in Europe.

The complaint is that under Articles 8 and 14 of the convention that the authorities continued to retain their fingerprints and cellular samples and DNA profiles after the Criminal proceedings against them had ended with an acquittal or had been dropped. Third parties were allowed appear in the matter to make submission on the question. “National council for Civil liberties (liberty) submitted case law and scientific material highlighting, inter alia, the highly sensitive nature of cellular samples and DNA profiles and the impact on private life arising from their retention by the authorities”

“57. Privacy International referred to certain core data protection rules and principles developed by the Council of Europe and insisted on their high relevance for the interpretation of the proportionality requirement enshrined in Article 8 of the Convention. It emphsised in particular the “strict period” recommended by Recommendation R (92) 1 for the storage of cellular samples and DNA profiles. It further pointed out a disproportionate representation on the United Kingdom national DNA data base of certain groups of population, notably youth, and the unfairness that situation might create. The use of data for familial testing and additional research purposes was also of concerned. Privacy international also provided a summary of comparative data on the law and practice of different countries with regard to DNA storage and

stressed the numerous restrictions and safeguards which existed in that respect.

The Court stated the General Principles.

“66. The Court recalls that the concept of “private life” is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see Pretty v the Untied Kingdom, no.2346/02, $33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person’s physical and social identity (See Milkulic v Croatia, No.53176/99, $ 53, ECHR 2002-1). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (See among other authorities, Ben said v the United Kingdom, no.44647/98 $ 57, ECHR 2003-1). Beyond a person’s name, his or her private and family life may include other means of personal identification and of linking to a family (see mutatis mutandis Burghartz v Switzerland, 22 February, 1994, $ 24, Series A no.280-B; and Unal Tekeli v Turkey, no.,29865/96, $ 42, ECHR 2004-X (extracts)). Information about the person’s health is an important element of private life (see Z v Finland, 25 February 1997, $ 71 Reports of Judgments and Decisions 1997-1).The Court furthermore considers that an individual’s ethnic identity must be regarded as another such element (see in particular Article 6 of the Data Protection Convention quoted in Paragraph 41 above, which lists personal data

revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz, cited above, opinion of the Commission, p.37, $ 47, and Friedl v Austria, judgment of 31 January 1995, series A no.305-B, opinion of the Commissioner, p.20$ 45). The concept of private life moreover includes elements relating to a person's right to their image (Sciacca v Italy, no.50774/99, $ 29 ECHR 2005-1)

Regarding protection of personal data the court said:

"103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, mutatis mutandis, Z., cited above, $ 95). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and 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 (see Article 5 of the Data Protection Convention and the preamble thereto and Principle 7 of Recommendations R(87)15 of the Committee of Minister regulating the use of personal data in the police sector). The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention). The above considerations are especially valid as regards the protection of special categories of more sensitive data (see Article 6 of the Data Protection Convention) and more particularly of DNA, information, which contains the persons genetic makeup of great importance to both the person concerned and his or her family (see Recommendation No. R (2)) of the committee of minorities on the use of analysis of DNA within the frame work of the criminal Justice system)

The Court held

“125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, are applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants’ right to respect for

private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism. Regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

"126. Accordingly, there has been a violation of Article 8 of the Convention in the present case.

After the Judgment of European Court of Human rights in S & Marper's case ECHR 30562/2004 & ECHR30566/04 Dt.4-12-2008, the question of retention of finger prints and DNA came up before the Supreme Court of England (House of Lords having been abolished on 1-10-2009). 2011 (3) All ER 193. R (on the application of GC v Metropolitan Police Commissioner. R (on the application of C) v Metropolitan Police Commissioner. The Head note conebly states the facts and the decison.

Police – powers – Fingerprints and DNA samples – Retention of fingerprints and DNA samples lawfully taken from persons who are not convicted – right to respect for private and family life – Policy of destruction of samples only in exceptional circumstances – Whether scheme of statute and policy compatible with right to respect for private life – Whether scheme unlawful – Police and Criminal Evidence

Act, 1984, s 64(1A) – Human Rights Act 1998, ss 6(1), (2)(b), 8(1), Sch 1, Pt I, art 8.

As originally enacted s 64 of the Police and Criminal Evidence Act 1984 (PACE) had provided that fingerprints and samples taken from a person in connection with the investigation of an offence had to be destroyed if the person was cleared of that offence or if the person was not suspected of having committed the offence. Section 64(1A) was enacted by the Criminal Justice and Police Act 2001. It provided; “Where – (a) fingerprints, impressions of footwear or samples are taken from a person in connection with the investigation of an offence...the fingerprints, impressions of footwear or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person from whom a body part came.’ The time limit for the retention of such data and procedure to regulate its destruction were addressed in guidelines issued by the Association of Chief Police Officer (the ACPO guidelines) which stated that chief officers had the discretion to authorize the deletion of any specific data entry on the police national database and were responsible for the authorization of the destruction of DNA and fingerprints associated with that specific entry It is suggested that this

discretion should only be exercised in exceptional cases.' GC was arrested in December, 2007 on suspicion of common assault. He denied the offence. A DNA sample and fingerprints were taken. He was later informed that no further action – would be taken. In March 2007 he requested the destruction of the data. The Metropolitan Police Commissioner refused to do so on the grounds that there were no exceptional circumstances within the meaning of the ACPO guidelines. In March 2009 C was arrested on suspicion of rape, harassment and fraud. His fingerprints and a DNA sample were taken. No further action was taken in respect of the harassment and fraud allegations; he was charged with rape. In the Crown Court the prosecution offered no evidence and C was acquitted. C requested the destruction of his data. The commissioner refused his request, informing C that his case was not 'exceptional' within the ACPO guidelines. GC and C issued proceedings for judicial review of the retention of their data on the grounds that following a decision of the European Court of Human Rights, its retention was incompatible with their rights to respect for private life under art b of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (as set out in Sch 1 to the Human Rights Act 1998). The Divisional Court held that an earlier decision of the House of Lords was binding on it, dismissed both claims for judicial review and granted a certificate for a 'leap frog' appeal to the Supreme

Court. It was common ground that the decision of the Court of Human Rights established that the indefinite retention of the claimants' data was an interference with their rights to respect for private life protected by art 8 of the convention. The Supreme Court therefore considered what remedy should be granted. Section 6(1) of the 1998 Act provided that it was unlawful for a public authority to act in a way which was incompatible with a convention right and s 6(2)(b) provided that s 6(1) did not apply to an act if the public authority had been acting so as to give effect to or enforce provisions of, or made under primary legislation which could not be read or given effect in a way which was compatible with the convention rights. Section 8(1) of the 1998 Act provided that in relation to any act of a public authority which the court found unlawful it could grant such relief or make such order as it considered just and appropriate. C submitted that the court should grant a declaration under s 8(1) that the retention of his biometric data was unlawful; GC submitted that the ACPO guidelines should be quashed and a reconsideration of the retention of his data should be ordered. The commissioner submitted that a declaration of incompatibility under s 6 of the 1998 Act should be granted on the bases that to interpret s 64(1A) of PACE as requiring police authorities to comply with art 8 would defeat the statutory purpose of establishing a scheme for the protection of the public interest free from the limits and protections required by art 8 and that Parliament could not

have intended to entrust the creation of a detailed scheme pursuant to s 64(1A) to the police subject only to the judicial review jurisdiction of the court as the creation of guidelines involved choices between different policy solutions which were for Parliament alone. The Secretary of State for the Home Department submitted that making a declaration of incompatibility was not necessary.

Lord Dyson SCJ stated: The Issue

"(15) It is common ground that, in the light of Marper ECtHR, the indefinite retention of the appellant's data is an interference with their rights to respect for private life protected by art 8 of the convention which, for the reasons given by the ECtHR, is not justified under art 8(2). It is agreed that Marper UK cannot stand. The issue that arises on these appeals is what remedy the court should grant in these circumstances.

"WHAT RELIEF, IF ANY, SHOULD BE GRANTED?

'The biometric data

(45) In deciding what relief to grant, it is important to have regard to the present state of play. As previously stated, Ch 1 of Pt 1 of the Protection of Freedoms Bill includes proposals along the lines of the Scottish model. The history of the varying responses to Marper ECtHR shows that it is not certain that it will be enacted. But we were told by Mr Eadie that it is the present intention of the government to bring the legislation into force later this year. In shaping the appropriate relief in

the present case, I consider that it is right to proceed on the basis that this is likely to happen, although not certain to do so.

“(46) In these circumstances, in my view it is appropriate to grant a declaration that the present ACPO guidelines (amended as they have been to exclude children under the age of ten), are unlawful because, as clearly demonstrated by Marper ECtHR, they are incompatible with the convention. It is important that, in such an important and sensitive area as the retention of biometric data by the police, the court reflects its decision by making formal.

“a order to declare what it considers to be the true legal position. But it is not necessary to go further. Section 8(1) OF THE 1998 act gives the court a wide discretion to grant such relief or remedy within its powers as it considers just and appropriate since Parliament is already seised of the matter, it is neither junior appropriate to make an order requiring a change in the legislative scheme within a specific period.

“b(47) The European Court of Human Right has recently decided that, where one of its judgments raises issues of general public importance and sensitivity, in respect of which the national authorities enjoy a discretionary area of judgment, it may be appropriate to leave the national legislature a reasonable period of time to address those issues: see Greens v UK App Nos 60041/08 and 60054/08 (23 November 2010, unreported) at paras 113-115. This is an obviously sensible approach. The

legislature must be allowed a reasonable time in which to produce a lawful solution to difficult problem.

"(48) Nor would it be just or appropriate to make an order for the destruction of data which it is possible (to put it no higher) it will be lawful to retain under the scheme which Parliament produces.

"(49) In these circumstances, the only order that should be made is to grant a declaration that the present APCP guidelines (as amended) are unlawful. If Parliament does not produce revised guidelines within a reasonable time, then the appellants will be able to seek judicial review of the continuing retention of their data under the unlawful ACPO guidelines and their claims will be likely to succeed.

CONCLUSION:

(52) For the reasons that I have given, I would allow the appeals and grant a declaration that the present APCO guidelines are unlawful because they are incompatible with art 8 of the convention. I would grant no other relief.

Lady Hale SCJ

Reiterated what she said in S & Marper's case.

USA

In Privacy Act of 1974 5USC 1 5529

Record is defined – section 2(4) states the term record means any item, collection or grouping of information about an individual that is maintained by an agency, including but not limited to his education, financial transaction, medical history and criminal or employment history and that contains his name or the identified number, symbol or other identifying particulars assigned to the individual, such as a finger or voice print or a photograph.

Section 13(b) states condition of disclosure.

No agency shall disclose any record which is contained in a system of records by any means of communication to any person or to any agency, except pursuant to a written request by or with the prior written consent of the individual to whom the record pertains, unless disclosure of the record would be…..

(1) To those officers and employees of the agency which maintains the record who have a need for the record in the performance of them duties.

(2) Requires under section 552 of the other subsections not necessary to mention.

USA

In Davis v Mississippi 394 US 721 = 22 Led (2) 676 held that evidence of Fingerprints obtained from the defendant for the second time when he was detained subsequently without a warrant issued by a judicial officer and without probable cause was inadmissible at his trial having been detained in violation of the fourth & fourteen amendment.. It does not admit of any exceptions. Kindly see also Joe Hays v Florida 470US 811 = 84 Led (2) 705.

Natural rights are those which pertain to a man in right of existence. Of this kind are all *Intellectual Rights or Rights of the Mind* and also those rights as an individual for his own comfort and happiness, which are not injurious to the natural rights of others. Every civil right has for its foundation some natural right pre-existing in the individuals.

The individuals themselves each in his own personal and sovereign right entered into a compact with each other to produce a Government, and this is the only mode in which Governments have a right to arise and the only principle on which they have a right to exist.

……..Paine – RIGHTS OF MAN.

The Aadhar destroyed the individual's right to privacy.

* * * * * * * * *

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION
New Delhi, the 11th April, 2011

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. **Short title and commencement —** (1) These rules may be called the **Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.**

(2) They shall come into force on the date of their publication in the Official Gazette.

2**. Definitions —** (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

(c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;

(d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(h) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

(i) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

4. Body corporate to provide policy for privacy and disclosure of information.— (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force..

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

the provider of information to such boy corporate or any other person acting on behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.

6. Disclosure of information.— (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

8. **Reasonable Security Practices and Procedures.**— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

CASE OF S. AND MARPER v. THE UNITED KINGDOM

(Applications nos. 30562/04 and 30566/04)

JUDGMENT

STRASBOURG

4 December 2008

This judgment is final but may be subject to editorial revision.

In the case of S. and Marper v. the United Kingdom,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Jean-Paul Costa, *President,*
Christos Rozakis,
Nicolas Bratza,
Peer Lorenzen,
Françoise Tulkens,
Josep Casadevall,
Giovanni Bonello,
Corneliu Bîrsan,
Nina Vajić,
Anatoly Kovler,
Stanislav Pavlovschi,
Egbert Myjer,
Danut÷ Jočien÷,
Ján Šikuta,
Mark Villiger,
Päivi Hirvelä,
Ledi Bianku, *judges,*

and Michael O'Boyle, *Deputy Registrar*,

Having deliberated in private on 27 February 2008 and on 12 November 2008,

Delivers the following judgment, which was adopted on the last mentioned date:

PROCEDURE

1. The case originated in two applications (nos. 30562/04 and 30566/04) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by two British nationals, Mr S. ("the first applicant") and Mr Michael Marper ("the second applicant"), on 16 August 2004. The President of the Grand Chamber acceded to the first applicant's request not to have his name disclosed (Rule 47 § 3 of the Rules of Court).

2. The applicants, who were granted legal aid, were represented by Mr P. Mahy of Messrs Howells, a solicitor practicing in Sheffield. The United Kingdom Government ("the Government") were represented by their Agent, Mr J. Grainger, Foreign and Commonwealth Office.

3. The applicants complained under Articles 8 and 14 that the authorities had continued to retain their fingerprints and cellular samples and DNA

profiles after the criminal proceedings against them had ended with an acquittal or had been discontinued.

4. The applications were allocated to the Fourth Section of the Court (Rule 52 § 1 of the Rules of Court). On 16 January 2007 they were declared admissible by a Chamber of that Section composed of the following judges: Josep Casadevall, *President*, Nicolas Bratza, Giovanni Bonello, Kristaq Traja, Stanislav Pavlovschi, Ján Šikuta, Päivi Hirvelä, and also of Lawrence Early, Section Registrar.

5. On 10 July 2007 the Chamber relinquished jurisdiction in favour of the Grand Chamber, neither party having objected to relinquishment (Article 30 of the Convention and Rule 72).

6. The composition of the Grand Chamber was determined according to the provisions of Article 27 §§ 2 and 3 of the Convention and Rule 24 of the Rules of Court.

7. The applicants and the Government each filed written memorials on the merits. In addition, third-party submissions were received from Ms Anna Fairclough on behalf of Liberty (the National Council for Civil Liberties) and from Covington and Burling LLP on behalf of Privacy International, who had been granted leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 2). Both parties replied to Liberty's submissions and the Government also replied to the comments by Privacy International (Rule 44 § 5).

8. A hearing took place in public in the Human Rights Building, Strasbourg, on 27 February 2008 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government*

Mrs	E. WILLMOTT,	*Agent*,
Mr	RABINDER SINGH QC,	
Mr	J. STRACHAN,	*Counsel*,
Mr	N. FUSSELL,	
Ms	P. MCFARLANE,	
Mr	M. PRIOR,	
Mr	S. BRAMBLE,	
Ms	E. REES,	
Mr	S. SEN,	*Advisers*,
Mr	D. GOURLEY,	
Mr	D. LOVEDAY,	*Observers*;

(b) *for the applicants*

Mr	S. CRAGG,	
Mr	A. SUTERWALLA,	*Counsel*,
Mr	P. MAHY,	*Solicitor*.

The Court heard addresses by Mr S. Cragg and Mr Rabinder Singh QC as well as their answers to questions put by the Court.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

9. The applicants were born in 1989 and 1963 respectively and live in Sheffield.

10. The first applicant, Mr S., was arrested on 19 January 2001 at the age of eleven and charged with attempted robbery. His fingerprints and DNA samples[1] were taken. He was acquitted on 14 June 2001.

11. The second applicant, Mr Michael Marper, was arrested on 13 March 2001 and charged with harassment of his partner. His fingerprints and DNA samples were taken. Before a pre-trial review took place, he and his partner had become reconciled, and the charge was not pressed. On 11 June 2001, the Crown Prosecution Service served a notice of discontinuance on the applicant's solicitors, and on 14 June the case was formally discontinued.

12. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused. The applicants applied for judicial review of the police decisions not to destroy the fingerprints and samples. On 22 March 2002 the Administrative Court (Rose LJ and Leveson J) rejected the application [[2002] EWHC 478 (Admin)].

13. On 12 September 2002 the Court of Appeal upheld the decision of the Administrative Court by a majority of two (Lord Woolf CJ and Waller LJ) to one (Sedley LJ) [[2003] EWCA Civ 1275]. As regards the necessity of retaining DNA samples, Lord Justice Waller stated:

> "... [F]ingerprints and DNA *profiles* reveal only limited personal information. The physical samples potentially contain very much greater and more personal and detailed information. The anxiety is that science may one day enable analysis of samples to go so far as to obtain information in relation to an individual's propensity to commit certain crime and be used for that purpose within the language of the present section [Section 82 of the Criminal Justice and Police Act 2001]. It might also be said that the law might be changed in order to allow the samples to be used for

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

> purposes other than those identified by the section. It might also be said that while samples are retained there is even now a risk that they will be used in a way that the law does not allow. So, it is said, the aims could be achieved in a less restrictive manner... Why cannot the aim be achieved by retention of the profiles without retention of the samples?
>
> The answer to [these] points is as I see it as follows. First the retention of samples permits (a) the checking of the integrity and future utility of the DNA database system; (b) a reanalysis for the upgrading of DNA profiles where new technology can improve the discriminating power of the DNA matching process; (c) reanalysis and thus an ability to extract other DNA markers and thus offer benefits in terms of speed, sensitivity and cost of searches of the database; (d) further analysis in investigations of alleged miscarriages of justice; and (e) further analysis so as to be able to identify any analytical or process errors. It is these benefits which must be balanced against the risks identified by Liberty. In relation to those risks, the position in any event is first that any change in the law will have to be itself Convention compliant; second any change in practice would have to be Convention compliant; and third unlawfulness must not be assumed. In my view thus the risks identified are not great, and such as they are they are outweighed by the benefits in achieving the aim of prosecuting and preventing crime."

14. Lord Justice Sedley considered that the power of a Chief Constable to destroy data which he would ordinarily retain had to be exercised in every case, however rare such cases might be, where he or she was satisfied on conscientious consideration that the individual was free of any taint of suspicion. He also noted that the difference between the retention of samples and DNA profiles was that the retention of samples would enable more information to be derived than had previously been possible.

15. On 22 July 2004 the House of Lords dismissed an appeal by the applicants. Lord Steyn, giving the lead judgment, noted the legislative history of section 64 (1A) of the Police and Criminal Evidence Act 1984 ("the PACE"), in particular the way in which it had been introduced by Parliament following public disquiet about the previous law, which had provided that where a person was not prosecuted or was acquitted of offences, the sample had to be destroyed and the information could not be used. In two cases, compelling DNA evidence linking one suspect to a rape and another to a murder had not been able to be used, as at the time the matches were made both defendants had either been acquitted or a decision made not to proceed for the offences for which the profiles had been obtained: as a result it had not been possible to convict either suspect.

16. Lord Steyn noted that the value of retained fingerprints and samples taken from suspects was considerable. He gave the example of a case in 1999, in which DNA information from the perpetrator of a crime was matched with that of "I" in a search of the national database. The sample from "I" should have been destroyed, but had not been. "I" had pleaded guilty to rape and was sentenced. If the sample had not been wrongly detained, the offender might have escaped detection.

17. Lord Steyn also referred to statistical evidence from which it appeared that almost 6,000 DNA profiles had been linked with crime-scene stain profiles which would have been destroyed under the former provisions. The offences involved included 53 murders, 33 attempted murders, 94 rapes, 38 sexual offences, 63 aggravated burglaries and 56 cases involving the supply of controlled drugs. On the basis of the existing records, the Home Office statistics estimated that there was a 40% chance that a crime-scene sample would be matched immediately with an individual's profile on the database. This showed that the fingerprints and samples which could now be retained had in the previous three years played a major role in the detection and prosecution of serious crime.

18. Lord Steyn also noted that the PACE dealt separately with the taking of fingerprints and samples, their retention and their use.

19. As to the Convention analysis, Lord Steyn inclined to the view that the mere retention of fingerprints and DNA samples did not constitute an interference with the right to respect for private life but stated that, if he were wrong in that view, he regarded any interference as very modest indeed. Questions of whether in the future retained samples could be misused were not relevant in respect of contemporary use of retained samples in connection with the detection and prosecution of crime. If future scientific developments required it, judicial decisions could be made, when the need occurred, to ensure compatibility with the Convention. The provision limiting the permissible use of retained material to "*purposes related to* the prevention or detection of crime ..." did not broaden the permitted use unduly, because it was limited by its context.

20. If the need to justify the modest interference with private life arose, Lord Steyn agreed with Lord Justice Sedley in the Court of Appeal that the purposes of retention – the prevention of crime and the protection of the right of others to be free from crime – were "provided for by law", as required by Article 8.

21. As to the justification for any interference, the applicants had argued that the retention of fingerprints and DNA samples created suspicion in respect of persons who had been acquitted. Counsel for the Home Secretary had contended that the aim of the retention had nothing to do with the past, that is, with the offence of which a person was acquitted, but that it was to assist in the investigation of offences in the future. The applicants would only be affected by the retention of the DNA samples if their profiles matched those found at the scene of a future crime. Lord Steyn saw five factors which led to the conclusion that the interference was proportionate to the aim: (i) the fingerprints and samples were kept only for the limited purpose of the detection, investigation and prosecution of crime; (ii) the fingerprints and samples were not of any use without a comparator fingerprint or sample from the crime scene; (iii) the fingerprints would not be made public; (iv) a person was not identifiable from the retained material

to the untutored eye, and (v) the resultant expansion of the database by the retention conferred enormous advantages in the fight against serious crime.

22. In reply to the contention that the same legislative aim could be obtained by less intrusive means, namely by a case-by-case consideration of whether or not to retain fingerprints and samples, Lord Steyn referred to Lord Justice Waller's comments in the Court of Appeal that "[i]f justification for retention is in any degree to be by reference to the view of the police on the degree of innocence, then persons who have been acquitted and have their samples retained can justifiably say this stigmatises or discriminates against me – I am part of a pool of acquitted persons presumed to be innocent, but I am treated as though I was not. It is not in fact in any way stigmatising someone who has been acquitted to say simply that samples lawfully obtained are retained as the norm, and it is in the public interest in its fight against crime for the police to have as large a database as possible".

23. Lord Steyn did not accept that the difference between samples and DNA profiles affected the position.

24. The House of Lords further rejected the applicants' complaint that the retention of their fingerprints and samples subjected them to discriminatory treatment in breach of Article 14 of the Convention when compared to the general body of persons who had not had their fingerprints and samples taken by the police in the course of a criminal investigation. Lord Steyn held that, even assuming that the retention of fingerprints and samples fell within the ambit of Article 8 so as to trigger the application of Article 14, the difference of treatment relied on by the applicants was not one based on "status" for the purposes of Article 14: the difference simply reflected the historical fact, unrelated to any personal characteristic, that the authorities already held the fingerprints and samples of the individuals concerned which had been lawfully taken. The applicants and their suggested comparators could not in any event be said to be in an analogous situation. Even if, contrary to his view, it was necessary to consider the justification for any difference in treatment, Lord Steyn held that such objective justification had been established: first, the element of legitimate aim was plainly present, as the increase in the database of fingerprints and samples promoted the public interest by the detection and prosecution of serious crime and by exculpating the innocent; secondly, the requirement of proportionality was satisfied, section 64 (1A) of the PACE objectively representing a measured and proportionate response to the legislative aim of dealing with serious crime.

25. Baroness Hale of Richmond disagreed with the majority considering that the retention of both fingerprint and DNA data constituted an interference by the State in a person's right to respect for his private life and thus required justification under the Convention. In her opinion, this was an aspect of what had been called informational privacy and there could be

little, if anything, more private to the individual than the knowledge of his genetic make-up. She further considered that the difference between fingerprint and DNA data became more important when it came to justify their retention as the justifications for each of these might be very different. She agreed with the majority that such justifications had been readily established in the applicants' cases.

II. RELEVANT DOMESTIC LAW AND MATERIALS

A. England and Wales

1. Police and Criminal Evidence Act 1984

26. The Police and Criminal Evidence Act 1984 (the PACE) contains powers for the taking of fingerprints (principally section 61) and samples (principally section 63). By section 61, fingerprints may only be taken without consent if an officer of at least the rank of superintendent authorises the taking, or if the person has been charged with a recordable offence or has been informed that he will be reported for such an offence. Before fingerprints are taken, the person must be informed that the prints may be the subject of a speculative search, and the fact of the informing must be recorded as soon as possible. The reason for the taking of the fingerprints is recorded in the custody record. Parallel provisions relate to the taking of samples (section 63).

27. As to the retention of such fingerprints and samples (and the records thereof), section 64 (1A) of the PACE was substituted by Section 82 of the Criminal Justice and Police Act 2001. It provides as follows:

> "Where - (a) fingerprints or samples are taken from a person in connection with the investigation of an offence, and (b) subsection (3) below does not require them to be destroyed, the fingerprints or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, or the conduct of a prosecution. ...
>
> (3) If - (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must except as provided in the following provisions of this Section be destroyed as soon as they have fulfilled the purpose for which they were taken.
>
> (3AA) Samples and fingerprints are not required to be destroyed under subsection (3) above if (a) they were taken for the purposes of the investigation of an offence of which a person has been convicted; and (b) a sample or, as the case may be, fingerprint was also taken from the convicted person for the purposes of that investigation."

28. Section 64 in its earlier form had included a requirement that if the person from whom the fingerprints or samples were taken in connection with the investigation was acquitted of that offence, the fingerprints and samples, subject to certain exceptions, were to be destroyed "as soon as practicable after the conclusion of the proceedings".

29. The subsequent use of materials retained under section 64 (1A) is not regulated by statute, other than the limitation on use contained in that provision. In *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91, the House of Lords had to consider whether it was permissible to use in evidence a sample which should have been destroyed under the then text of section 64 the PACE. The House considered that the prohibition on the use of an unlawfully retained sample "for the purposes of any investigation" did not amount to a mandatory exclusion of evidence obtained as a result of a failure to comply with the prohibition, but left the question of admissibility to the discretion of the trial judge.

2. Data Protection Act 1998

30. The Data Protection Act was adopted on 16 July 1998 to give effect to the Directive 95/46/EC of the European Parliament and of the Council dated 24 October 1995 (see paragraph 50 below). Under the Data Protection Act "personal data" means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (section 1). "Sensitive personal data" means personal data consisting, *inter alia*, of information as to the racial or ethnic origin of the data subject, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings (section 2).

31. The Act stipulates that the processing of personal data is subject to eight data protection principles listed in Schedule 1. Under the first principle personal data shall be processed fairly and lawfully and, in particular shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. Schedule 2 contains a detailed list of conditions, and provides *inter alia* that the processing of any personal data is necessary for the administration of justice or for the exercise of any other functions of a public nature exercised in the public interest by any person (§5(a) and (d)). Schedule 3 contains a more detailed list of conditions, including that the processing of sensitive personal data is necessary for the purpose of, or in connection with, any legal proceedings (§6(a)), or for the administration of

justice (§7(a)), and is carried out with appropriate safeguards for the rights and freedoms of data subjects (§4(b)). Section 29 notably provides that personal data processed for the prevention or detection of crime are exempt from the first principle except to the extent to which it requires compliance with the conditions in Schedules 2 and 3. The fifth principle stipulates that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

32. The Information Commissioner created pursuant to the Act (as amended) has an independent duty to promote the following of good practice by data controllers and has power to make orders ("enforcement notices") in this respect (section 40). The Act makes it a criminal offence not to comply with an enforcement notice (section 47) or to obtain or disclose personal data or information contained therein without the consent of the data controller (section 55). Section 13 affords a right to claim damages in the domestic courts in respect of contraventions of the Act.

3. Retention Guidelines for Nominal Records on the Police National Computer 2006

33. A set of guidelines for the retention of fingerprint and DNA information is contained in the Retention Guidelines for Nominal Records on the Police National Computer 2006 drawn up by the Association of Chief Police Officers in England and Wales. The Guidelines are based on a format of restricting access to the Police National Computer (PNC) data, rather than the deletion of that data. They recognise that their introduction may thus have implications for the business of the non-police agencies with which the police currently share PNC data.

34. The Guidelines set various degrees of access to the information contained on the PNC through a process of "stepping down" access. Access to information concerning persons who have not been convicted of an offence is automatically "stepped down" so that this information is only open to inspection by the police. Access to information about convicted persons is likewise "stepped down" after the expiry of certain periods of time ranging from 5 to 35 years, depending on the gravity of the offence, the age of the suspect and the sentence imposed. For certain convictions the access will never be "stepped down".

35. Chief Police Officers are the Data Controllers of all PNC records created by their force. They have the discretion in exceptional circumstances to authorise the deletion of any conviction, penalty notice for disorder, acquittal or arrest histories "owned" by them. An "exceptional case procedure" to assist Chief Officers in relation to the exercise of this discretion is set out in Appendix 2. It is suggested that exceptional cases are rare by definition and include those where the original arrest or sampling was unlawful or where it is established beyond doubt that no offence

existed. Before deciding whether a case is exceptional, the Chief Officer is instructed to seek advice from the DNA and Fingerprint Retention Project.

B. Scotland

36. Under the 1995 Criminal Procedure Act of Scotland, as subsequently amended, the DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. A recent qualification provides that biological samples and profiles may be retained for three years, if the arrestee is suspected of certain sexual or violent offences even if a person is not convicted (section 83 of the 2006 Act, adding section 18A to the 1995 Act.). Thereafter, samples and information are required to be destroyed unless a Chief Constable applies to a Sheriff for a two-year extension.

C. Northern Ireland

37. The Police and Criminal Evidence Order of Northern Ireland 1989 was amended in 2001 in the same way as the PACE applicable in England and Wales. The relevant provisions currently governing the retention of fingerprint and DNA data in Northern Ireland are identical to those in force in England and Wales (see paragraph 27 above).

D. Nuffield Council on Bioethics' report[1]

38. According to a recent report by the Nuffield Council on Bioethics, the retention of fingerprints, DNA profiles and biological samples is generally more controversial than the taking of such bioinformation, and the retention of biological samples raises greater ethical concerns than digitised DNA profiles and fingerprints, given the differences in the level of information that could be revealed. The report referred in particular to the lack of satisfactory empirical evidence to justify the present practice of retaining indefinitely fingerprints, samples and DNA profiles from all those arrested for a recordable offence, irrespective of whether they were subsequently charged or convicted. The report voiced particular concerns at the policy of permanently retaining the bioinformation of minors, having regard to the requirements of the 1989 UN Convention on the Rights of the Child.

---

[1] The Nuffield Council on Bioethics is an independent expert body composed of clinicians, lawyers, philosophers, scientists and theologians established by the Nuffield Foundation in 1991. The present report was published on 18 September 2007 under the following title "The forensic use of bioinformation: ethical issues"

39. The report also expressed concerns at the increasing use of the DNA data for familial searching, inferring ethnicity and non-operational research. Familial searching is the process of comparing a DNA profile from a crime scene with profiles stored on the national database, and prioritising them in terms of 'closeness' to a match. This allowed identifying possible genetic relatives of an offender. Familial searching might thus lead to revealing previously unknown or concealed genetic relationships. The report considered the use of the DNA data base in searching for relatives as particularly sensitive.

40. The particular combination of alleles[1] in a DNA profile can furthermore be used to assess the most likely ethnic origin of the donor. Ethnic inferring through DNA profiles was possible as the individual "ethnic appearance" was systematically recorded on the data base: when taking biological samples, police officers routinely classified suspects into one of seven "ethnical appearance" categories. Ethnicity tests on the data base might thus provide inferences for use during a police investigation in order for example to help reduce a 'suspect pool' and to inform police priorities. The report noted that social factors and policing practices lead to a disproportionate number of people from black and ethnic minority groups being stopped, searched and arrested by the police, and hence having their DNA profiles recorded; it therefore voiced concerns that inferring ethnic identity from biological samples might reinforce racist views of propensity to criminality.

III. RELEVANT NATIONAL AND INTERNATIONAL MATERIAL

A. Council of Europe texts

41. The Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which entered into force for the United Kingdom on 1 December 1987, defines "personal data" as any information relating to an identified or identifiable individual ("data subject"). The Convention provides *inter alia*:

> "Article 5 – Quality of data
>
> Personal data undergoing automatic processing shall be: ...

[1] Allele is one of two or more alternative forms of a particular gene. Different alleles may give rise to different forms of the characteristic for which the gene codes (*World Encyclopedia. Philip's, 2008. Oxford Reference Online. Oxford University Press*).

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

...

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. (...)

Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."

42. Recommendation No. R(87)15 regulating the use of personal data in the police sector (adopted on 17 September 1987) states, *inter alia*:

"Principle 2 – Collection of data

2.1 The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation. ...

Principle 3 - Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law....

Principle 7 - Length of storage and updating of data

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data."

43. Recommendation No. R(92)1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system (adopted on 10 February 1992) states, *inter alia*:

"3. *Use of samples and information derived therefrom*

Samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes. ...

Samples taken for DNA analysis and the information so derived may be needed for research and statistical purposes. Such uses are acceptable provided the identity of the individual cannot be ascertained. Names or other identifying references must therefore be removed prior to their use for these purposes.

4. *Taking of samples for DNA analysis*

The taking of samples for DNA analysis should only be carried out in circumstances determined by the domestic law; it being understood that in some states this may necessitate specific authorisation from a judicial authority...

8. *Storage of samples and data*

Samples or other body tissue taken from individuals for DNA analysis should not be kept after the rendering of the final decision in the case for which they were used, unless it is necessary for purposes directly linked to those for which they were collected.

Measures should be taken to ensure that the results of DNA analysis are deleted when it is no longer necessary to keep it for the purposes for which it was used. The results of DNA analysis and the information so derived may, however, be retained where the individual concerned has been convicted of serious offences against the life, integrity or security of persons. In such cases strict storage periods should be defined by domestic law.

Samples and other body tissues, or the information derived from them, may be stored for longer periods:

- when the person so requests; or

- when the sample cannot be attributed to an individual, for example when it is found at the scene of a crime;

Where the security of the state is involved, the domestic law of the member state may permit retention of the samples, the results of DNA analysis and the information so derived even though the individual concerned has not been charged or convicted of an offence. In such cases strict storage periods should be defined by domestic law. ..."

44. The Explanatory Memorandum to the Recommendation stated, as regards item 8:

"47. The working party was well aware that the drafting of Recommendation 8 was a delicate matter, involving different protected interests of a very difficult nature. It was necessary to strike the right balance between these interests. Both the European Convention on Human Rights and the Data Protection Convention provide exceptions for the interests of the suppression of criminal offences and the protection of the rights

and freedoms of third parties. However, the exceptions are only allowed to the extent that they are compatible with what is necessary in a democratic society. ...

49. Since the primary aim of the collection of samples and the carrying out of DNA analysis on such samples is the identification of offenders and the exoneration of suspected offenders, the data should be deleted once persons have been cleared of suspicion. The issue then arises as to how long the DNA findings and the samples on which they were based can be stored in the case of a finding of guilt.

50. The general rule should be that the data are deleted when they are no longer necessary for the purposes for which they were collected and used. This would in general be the case when a final decision has been rendered as to the culpability of the offender. By 'final decision' the CAHBI thought that this would normally, under domestic law, refer to a judicial decision. However, the working party recognised that there was a need to set up data bases in certain cases and for specific categories of offences which could be considered to constitute circumstances warranting another solution, because of the seriousness of the offences. The working party came to this conclusion after a thorough analysis of the relevant provisions in the European Convention on Human Rights, the Data Protection Convention and other legal instruments drafted within the framework of the Council of Europe. In addition, the working party took into consideration that all member states keep a criminal record and that such record may be used for the purposes of the criminal justice system... It took into account that such an exception would be permissible under certain strict conditions:

- when there has been a conviction;

- when the conviction concerns a serious criminal offence against the life, integrity and security of a person;

- the storage period is limited strictly;

- the storage is defined and regulated by law;

- the storage is subject to control by Parliament or an independent supervisory body..."

B. Law and practice in the Council of Europe member States

45. According to the information provided by the parties or otherwise available to the Court, a majority of the Council of Europe member States allow the compulsory taking of fingerprints and cellular samples in the context of criminal proceedings. At least 20 member States make provision for the taking of DNA information and storing it on national data bases or in other forms (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland[1], Italy[1], Latvia,

[1] The law and practice in Ireland are presently governed by the Criminal Justice (Forensic Evidence) Act 1990. A new Bill has been approved by the Government with a view to

Luxembourg, the Netherlands, Norway, Poland, Spain, Sweden and Switzerland). This number is steadily increasing.

46. In most of these countries (including Austria, Belgium, Finland, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Spain and Sweden), the taking of DNA information in the context of criminal proceedings is not systematic but limited to some specific circumstances and/or to more serious crimes, notably those punishable by certain terms of imprisonment.

47. The United Kingdom is the only member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued. Five States (Belgium, Hungary, Ireland, Italy and Sweden) require such information to be destroyed *ex officio* upon acquittal or the discontinuance of the criminal proceedings. Ten other States apply the same general rule with certain very limited exceptions: Germany, Luxembourg and the Netherlands allow such information to be retained where suspicions remain about the person or if further investigations are needed in a separate case; Austria permits its retention where there is a risk that the suspect will commit a dangerous offence and Poland does likewise in relation to certain serious crimes; Norway and Spain allow the retention of profiles if the defendant is acquitted for lack of criminal accountability; Finland and Denmark allow retention for 1 and 10 years respectively in the event of an acquittal and Switzerland for 1 year when proceedings have been discontinued. In France DNA profiles can be retained for 25 years after an acquittal or discharge; during this period the public prosecutor may order their earlier deletion, either on his or her own motion or upon request, if their retention has ceased to be required for the purposes of identification in connection with a criminal investigation. Estonia and Latvia also appear to allow the retention of DNA profiles of suspects for certain periods after acquittal.

48. The retention of DNA profiles of convicted persons is allowed, as a general rule, for limited periods of time after the conviction or after the convicted person's death. The United Kingdom thus also appears to be the only member State expressly to allow the systematic and indefinite retention of both profiles and samples of convicted persons.

49. Complaint mechanisms before data-protection monitoring bodies and/or before courts are available in most of the member States with regard to decisions to take celular samples or retain samples or DNA profiles.

---

extending the use and storage of DNA information in a national database. The Bill has not yet been approved by Parliament.

[1] The Legislative Decree of 30 October 2007 establishing a national DNA database was approved by the Italian Government and the Senate. However, the Decree eventually expired without having been formally converted into a Statute as a mistake in the drafting was detected. A corrected version of the decree is expected to be issued in 2008.

C. European Union

50. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides that the object of national laws on the processing of personal data is notably to protect the right to privacy as recognised both in Article 8 of the European Convention on Human Rights and in the general principles of Community law. The Directive sets out a number of principles in order to give substance to and amplify those contained in the Data Protection Convention of the Council of Europe. It allows Member States to adopt legislative measures to restrict the scope of certain obligations and rights provided for in the Directive when such a restriction constitutes notably a necessary measure for the prevention, investigation, detection and prosecution of criminal offences (Article 13).

51. The Prüm Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, which was signed by several members of the European Union on 27 May 2005, sets out rules for the supply of fingerprinting and DNA data to other Contracting Parties and their automated checking against their relevant data bases. The Convention provides *inter alia*:

> "Article 35 – Purpose
>
> 2. ... The Contracting Party administering the file may process the data supplied (...) solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording... The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned [above]."

52. Article 34 guarantees a level of protection of personal data at least equal to that resulting from the Data Protection Convention and requires the Contracting Parties to take into account Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe.

53. The Council framework decision of 24 June 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters states *inter alia*:

> "Article 5
>
> Establishment of time-limits for erasure and review
>
> Appropriate time-limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time-limits are observed."

D. Case-law in other jurisdictions

54. In the case of *R v. RC* [[2005] 3 S.C.R. 99, 2005 SCC 61] the Supreme Court of Canada considered the issue of retaining a juvenile first-time offender's DNA sample on the national data bank. The court upheld the decision by a trial judge who had found, in the light of the principles and objects of youth criminal justice legislation, that the impact of the DNA retention would be grossly disproportionate. In his opinion, Fish J. observed:

> "Of more concern, however, is the impact of an order on an individual's informational privacy interests. In R. v. Plant, [1993] 3 S.C.R. 281, at p. 293, the Court found that s. 8 of the Charter protected the 'biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state'. An individual's DNA contains the 'highest level of personal and private information': S.A.B., at para. 48. Unlike a fingerprint, it is capable of revealing the most intimate details of a person's biological makeup. ... The taking and retention of a DNA sample is not a trivial matter and, absent a compelling public interest, would inherently constitute a grave intrusion on the subject's right to personal and informational privacy."

E. UN Convention on the Rights of the Child of 1989

55. Article 40 of the UN Convention on the Rights of the Child of 20 November 1989 states the right of every child alleged as, accused of, or recognised as having infringed the penal law to be treated in a manner consistent with the promotion of the child's sense of dignity and worth, which reinforces the child's respect for the human rights and fundamental freedoms of others and which takes into account the child's age and the desirability of promoting the child's reintegration and the child's assuming a constructive role in society.

IV. THIRD PARTIES' SUBMISSIONS

56. The National Council for Civil Liberties ("Liberty") submitted case-law and scientific material highlighting, *inter alia*, the highly sensitive nature of cellular samples and DNA profiles and the impact on private life arising from their retention by the authorities.

57. Privacy International referred to certain core data-protection rules and principles developed by the Council of Europe and insisted on their high relevance for the interpretation of the proportionality requirement enshrined in Article 8 of the Convention. It emphasised in particular the "strict periods" recommended by Recommendation R (92) 1 for the storage of cellular samples and DNA profiles. It further pointed out a disproportionate representation on the United Kingdom national DNA data base of certain groups of population, notably youth, and the unfairness that

situation might create. The use of data for familial testing and additional research purposes was also of concern. Privacy International also provided a summary of comparative data on the law and practice of different countries with regard to DNA storage and stressed the numerous restrictions and safeguards which existed in that respect.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

58. The applicants complained under Article 8 of the Convention about the retention of their fingerprints, cellular samples and DNA profiles pursuant to section 64 (1A) of the Police and Criminal Evidence Act 1984 ("the PACE"). Article 8 provides, so far as relevant, as follows:

> "1. Everyone has the right to respect for his private ... life ...
>
> 2. 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 ... for the prevention of disorder or crime..."

A. Existence of an interference with private life

59. The Court will first consider whether the retention by the authorities of the applicants' fingerprints, DNA profiles and cellular samples constitutes an interference in their private life.

1. The parties' submissions

(a) The applicants

60. The applicants submitted that the retention of their fingerprints, cellular samples and DNA profiles interfered with their right to respect for private life as they were crucially linked to their individual identity and concerned a type of personal information that they were entitled to keep within their control. They recalled that the initial taking of such bio-information had consistently been held to engage Article 8 and submitted that their retention was more controversial given the wealth of private information that became permanently available to others and thus came out of the control of the person concerned. They stressed in particular the social stigma and psychological implications provoked by such retention in the case of children, which made the interference with the right to private life all the more pressing in respect of the first applicant.

61. They considered that the Convention organs' case-law supported this contention, as did a recent domestic decision of the Information Tribunal (*Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v. the Information Commissioner,* [2005] UK IT EA 2005 0010 (12 October 2005), 173). The latter decision relied on the speech of Baroness Hale of Richmond in the House of Lords (see paragraph 25 above) and followed in substance her finding when deciding a similar question about the application of Article 8 to the retention of conviction data.

62. They further emphasised that retention of cellular samples involved an even greater degree of interference with Article 8 rights as they contained full genetic information about a person including genetic information about his or her relatives. It was of no significance whether information was actually extracted from the samples or caused a detriment in a particular case as an individual was entitled to a guarantee that such information which fundamentally belonged to him would remain private and not be communicated or accessible without his permission.

(b) The Government

63. The Government accepted that fingerprints, DNA profiles and samples were "personal data" within the meaning of the Data Protection Act in the hands of those who can identify the individual. They considered, however, that the mere retention of fingerprints, DNA profiles and samples for the limited use permitted under section 64 of the PACE did not fall within the ambit of the right to respect for private life under Article 8 § 1 of the Convention. Unlike the initial taking of this data, their retention did not interfere with the physical and psychological integrity of the persons; nor did it breach their right to personal development, to establish and develop relationships with other human beings or the right to self-determination.

64. The Government submitted that the applicants' real concerns related to fears about the future uses of stored samples, to anticipated methods of analysis of DNA material and to potential intervention with the private life of individuals through active surveillance. It emphasised in this connection that the permitted extent of the use of the material was clearly and expressly limited by the legislation, the technological processes of DNA profiling and the nature of the DNA profile extracted.

65. The profile was merely a sequence of numbers which provided a means of identifying a person against bodily tissue, containing no materially intrusive information about an individual or his personality. The DNA database was a collection of such profiles which could be searched using material from a crime scene and a person would be identified only if and to the extent that a match was obtained against the sample. Familial searching through partial matches only occurred in very rare cases and was subject to very strict controls. Fingerprints, DNA profiles and samples were neither susceptible to any subjective commentary nor provided any information

about a person's activities and thus presented no risk to affect the perception of an individual or affect his or her reputation. Even if such retention were capable of falling within the ambit of Article 8 § 1 the extremely limited nature of any adverse effects rendered the retention not sufficiently serious to constitute an interference.

2. The Court's assessment

(a) General principles

66. The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III, and *Y.F. v. Turkey*, no. 24209/94, § 33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person's physical and social identity (see *Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002-I). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other authorities, *Bensaid v. the United Kingdom*, no. 44599/98, § 47, ECHR 2001-I with further references, and *Peck v. the United Kingdom*, no. 44647/98, § 57, ECHR 2003-I). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see *mutatis mutandis Burghartz v. Switzerland*, 22 February 1994, § 24, Series A no. 280-B; and *Ünal Tekeli v. Turkey*, no. 29865/96, § 42, ECHR 2004-X (extracts)). Information about the person's health is an important element of private life (see *Z. v. Finland*, 25 February 1997, § 71, *Reports of Judgments and Decisions* 1997-I). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see in particular Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, *Burghartz*, cited above, opinion of the Commission, p. 37, § 47, and *Friedl v. Austria*, judgment of 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). The concept of private life moreover includes elements relating to a person's right to their image (*Sciacca v. Italy*, no. 50774/99, § 29, ECHR 2005-I).

67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden,* 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (*Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II). However, in determining whether the personal information retained by the authorities involves any of

the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see, *mutatis mutandis*, *Friedl*, cited above, §§49-51, and *Peck v. the United Kingdom*, cited above, § 59).

(b) Application of the principles to the present case

68. The Court notes at the outset that all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. The Government accepted that all three categories are "personal data" within the meaning of the Data Protection Act 1998 in the hands of those who are able to identify the individual.

69. The Convention organs have already considered in various circumstances questions relating to the retention of such personal data by the authorities in the context of criminal proceedings. As regards the nature and scope of the information contained in each of these three categories of data, the Court has distinguished in the past between the retention of fingerprints and the retention of cellular samples and DNA profiles in view of the stronger potential for future use of the personal information contained in the latter (see *Van der Velden v. the Netherlands* (dec.), no. 29514/05, ECHR 2006-...). The Court considers it appropriate to examine separately the question of interference with the applicants' right to respect for their private lives by the retention of their cellular samples and DNA profiles on the one hand, and of their fingerprints on the other.

(i) Cellular samples and DNA profiles

70. In *Van der Velden,* the Court considered that, given the use to which cellular material in particular could conceivably be put in the future, the systematic retention of that material was sufficiently intrusive to disclose interference with the right to respect for private life (see *Van der Velden* cited above). The Government criticised that conclusion on the ground that it speculated on the theoretical future use of samples and that there was no such interference at present.

71. The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways

or in a manner which cannot be anticipated with precision today. Accordingly, the Court does not find any sufficient reason to depart from its finding in the *Van der Velden* case.

72. Legitimate concerns about the conceivable use of cellular material in the future are not, however, the only element to be taken into account in the determination of the present issue. In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. In this respect the Court concurs with the opinion expressed by Baroness Hale in the House of Lords (see paragraph 25 above).

73. Given the nature and the amount of personal information contained in cellular samples, their retention *per se* must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see *Amann* cited above, § 69).

74. As regards DNA profiles themselves, the Court notes that they contain a more limited amount of personal information extracted from cellular samples in a coded form. The Government submitted that a DNA profile is nothing more than a sequence of numbers or a bar-code containing information of a purely objective and irrefutable character and that the identification of a subject only occurs in case of a match with another profile in the database. They also submitted that, being in coded form, computer technology is required to render the information intelligible and that only a limited number of persons would be able to interpret the data in question.

75. The Court observes, nonetheless, that the profiles contain substantial amounts of unique personal data. While the information contained in the profiles may be considered objective and irrefutable in the sense submitted by the Government, their processing through automated means allows the authorities to go well beyond neutral identification. The Court notes in this regard that the Government accepted that DNA profiles could be, and indeed had in some cases been, used for familial searching with a view to identifying a possible genetic relationship between individuals. They also accepted the highly sensitive nature of such searching and the need for very strict controls in this respect. In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals (see paragraph 39 above) is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attached thereto and the likelihood of detriment in a particular case are immaterial in

this respect (see *Amann* cited above, § 69). This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.

76. The Court further notes that it is not disputed by the Government that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are in fact used in police investigations (see paragraph 40 above). The possibility the DNA profiles create for inferences to be drawn as to ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life. This conclusion is consistent with the principle laid down in the Data Protection Convention and reflected in the Data Protection Act that both list personal data revealing ethnic origin among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 30-31 and 41 above).

77. In view of the foregoing, the Court concludes that the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention.

(ii) Fingerprints

78. It is common ground that fingerprints do not contain as much information as either cellular samples or DNA profiles. The issue of alleged interference with the right to respect for private life caused by their retention by the authorities has already been considered by the Convention organs.

79. In *McVeigh*, the Commission first examined the issue of the taking and retention of fingerprints as part of a series of investigative measures. It accepted that at least some of the measures disclosed an interference with the applicants' private life, while leaving open the question of whether the retention of fingerprints alone would amount to such interference (*McVeigh, O'Neill and Evans* (no. 8022/77, 8025/77 and 8027/77, Report of the Commission of 18 March 1981, DR 25, p.15, § 224).

80. In *Kinnunen,* the Commission considered that fingerprints and photographs retained following the applicant's arrest did not constitute an interference with his private life as they did not contain any subjective appreciations which called for refutation. The Commission noted, however, that the data at issue had been destroyed nine years later at the applicant's request (*Kinnunen v. Finland*, no. 24950/94, Commission decision of 15 May 1996).

81. Having regard to these findings and the questions raised in the present case, the Court considers it appropriate to review this issue. It notes at the outset that the applicants' fingerprint records constitute their personal data (see paragraph 68 above) which contain certain external identification

features much in the same way as, for example, personal photographs or voice samples.

82. In *Friedl,* the Commission considered that the retention of anonymous photographs that have been taken at a public demonstration did not interfere with the right to respect for private life. In so deciding, it attached special weight to the fact that the photographs concerned had not been entered in a data-processing system and that the authorities had taken no steps to identify the persons photographed by means of data processing (see *Friedl* cited above, §§ 49-51).

83. In *P.G. and J.H.*, the Court considered that the recording of data and the systematic or permanent nature of the record could give rise to private-life considerations even though the data in question may have been available in the public domain or otherwise. The Court noted that a permanent record of a person's voice for further analysis was of direct relevance to identifying that person when considered in conjunction with other personal data. It accordingly regarded the recording of the applicants' voices for such further analysis as amounting to interference with their right to respect for their private lives (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 59-60, ECHR 2001-IX).

84. The Court is of the view that the general approach taken by the Convention organs in respect of photographs and voice samples should also be followed in respect of fingerprints. The Government distinguished the latter by arguing that they constituted neutral, objective and irrefutable material and, unlike photographs, were unintelligible to the untutored eye and without a comparator fingerprint. While true, this consideration cannot alter the fact that fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant.

85. The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.

86. In the instant case, the Court notes furthermore that the applicants' fingerprints were initially taken in criminal proceedings and subsequently recorded on a nationwide database with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes. It is accepted in this regard that, because of the information they contain, the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints. However, the Court, like Baroness Hale (see paragraph 25 above), considers that, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in

determining the question of justification, the retention of fingerprints constitutes an interference with the right to respect for private life.

B. Justification for the interference

1. The parties' submissions

(a) The applicants

87. The applicants argued that the retention of fingerprints, cellular samples and DNA profiles was not justified under the second paragraph of Article 8. The Government were given a very wide remit to use samples and DNA profiles notably for "purposes related to the prevention or detection of crime", "the investigation of an offence" or "the conduct of a prosecution". These purposes were vague and open to abuse as they might in particular lead to the collation of detailed personal information outside the immediate context of the investigation of a particular offence. The applicants further submitted that there were insufficient procedural safeguards against misuse or abuse of the information. Records on the PNC were not only accessible to the police, but also to 56 non-police bodies, including Government agencies and departments, private groups such as British Telecom and the Association of British Insurers, and even certain employers. Furthermore, the PNC was linked to the Europe-wide "Schengen Information System". Consequently, their case involved a very substantial and controversial interference with the right to private life, as notably illustrated by ongoing public debate and disagreement about the subject in the United Kingdom. Contrary to the assertion of the Government, the applicants concluded that the issue of the retention of this material was of great individual concern and the State had a narrow margin of appreciation in this field.

88. The applicants contended that the indefinite retention of fingerprints, cellular samples and DNA profiles of unconvicted persons could not be regarded as "necessary in a democratic society" for the purpose of preventing crime. In particular, there was no justification at all for the retention of cellular samples following the original generation of the DNA profile; nor had the efficacy of the profiles' retention been convincingly demonstrated since the high number of DNA matches relied upon by the Government was not shown to have led to successful prosecutions. Likewise, in most of the specific examples provided by the Government the successful prosecution had not been contingent on the retention of the records and in certain others the successful outcome could have been achieved through more limited retention in time and scope.

89. The applicants further submitted that the retention was disproportionate because of its blanket nature irrespective of the offences

involved, the unlimited period, the failure to take account of the applicants' circumstances and the lack of an independent decision-making process or scrutiny when considering whether or not to order retention. They further considered the retention regime to be inconsistent with the Council of Europe's guidance on the subject. They emphasised, finally, that retention of the records cast suspicion on persons who had been acquitted or discharged of crimes, thus implying that they were not wholly innocent. The retention thus resulted in stigma which was particularly detrimental to children as in the case of S. and to members of certain ethnic groups over-represented on the database.

(b) The Government

90. The Government submitted that any interference resulting from the retention of the applicants' fingerprints, cellular samples and DNA profiles was justified under the second paragraph of Article 8. It was in accordance with the law as expressly provided for, and governed by section 64 of the PACE, which set out detailed powers and restrictions on the taking of fingerprints and samples and clearly stated that they would be retained by the authorities regardless of the outcome of the proceedings in respect of which they were taken. The exercise of the discretion to retain fingerprints and samples was also, in any event, subject to the normal principles of law regulating discretionary power and to judicial review.

91. The Government further stated that the interference was necessary and proportionate for the legitimate purpose of the prevention of disorder or crime and/or the protection of the rights and freedoms of others. It was of vital importance that law enforcement agencies took full advantage of available techniques of modern technology and forensic science in the prevention, investigation and detection of crime for the interests of society generally. They submitted that the retained material was of inestimable value in the fight against crime and terrorism and the detection of the guilty and provided statistics in support of this view. They emphasised that the benefits to the criminal-justice system were enormous, not only permitting the detection of the guilty but also eliminating the innocent from inquiries and correcting and preventing miscarriages of justice.

92. As at 30 September 2005, the National DNA database held 181,000 profiles from individuals who would have been entitled to have those profiles destroyed before the 2001 amendments. 8,251 of those were subsequently linked with crime-scene stains which involved 13,079 offences, including 109 murders, 55 attempted murders, 116 rapes, 67 sexual offences, 105 aggravated burglaries and 126 offences of the supply of controlled drugs.

93. The Government also submitted specific examples of use of DNA material for successful investigation and prosecution in some eighteen specific cases. In ten of these cases the DNA profiles of suspects matched

some earlier unrelated crime-scene stains retained on the database, thus allowing successful prosecution for those earlier crimes. In another case, two suspects arrested for rape were eliminated from the investigation as their DNA profiles did not match the crime-scene stain. In two other cases the retention of DNA profiles of the persons found guilty of certain minor offences (disorder and theft) led to establishing their involvement in other crimes committed later. In one case the retention of a suspect's DNA profile following an alleged immigration offence helped his extradition to the United Kingdom a year later when he was identified by one of his victims as having committed rape and murder. Finally, in four cases DNA profiles retained from four persons suspected but not convicted of certain offences (possession of offensive weapons, violent disorder and assault) matched the crime-scene stains collected from victims of rape up to two years later.

94. The Government contended that the retention of fingerprints, cellular samples and DNA profiles could not be regarded as excessive since they were kept for specific limited statutory purposes and stored securely and subject to the safeguards identified. Their retention was neither warranted by any degree of suspicion of the applicants' involvement in a crime or propensity to crime nor directed at retaining records in respect of investigated alleged offences in the past. The records were retained because the police had already been lawfully in possession of them, and their retention would assist in the future prevention and detection of crime in general by increasing the size of the database. Retention resulted in no stigma and produced no practical consequence for the applicants unless the records matched a crime-scene profile. A fair balance was thus struck between individual rights and the general interest of the community and fell within the State's margin of appreciation.

2. The Court's assessment

(a) In accordance with the law

95. The Court recalls its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise (see *Malone v. the United Kingdom*, 2 August 1984, §§ 66-68, Series A no. 82; *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V; and *Amann* cited above, § 56).

96. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed (*Hasan and Chaush v. Bulgaria* [GC], no. 30985/96, § 84, ECHR 2000-XI, with further references).

97. The Court notes that section 64 of the PACE provides that the fingerprints or samples taken from a person in connection with the investigation of an offence may be retained after they have fulfilled the purposes for which they were taken (see paragraph 27 above). The Court agrees with the Government that the retention of the applicants' fingerprint and DNA records had a clear basis in the domestic law. There is also clear evidence that these records are retained in practice save in exceptional circumstances. The fact that chief police officers have power to destroy them in such rare cases does not make the law insufficiently certain from the point of view of the Convention.

98. As regards the conditions attached to and arrangements for the storing and use of this personal information, section 64 is far less precise. It provides that retained samples and fingerprints must not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

99. The Court agrees with the applicants that at least the first of these purposes is worded in rather general terms and may give rise to extensive interpretation. It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see, *mutatis mutandis*, *Kruslin v. France*, 24 April 1990, §§ 33 and 35, Series A no. 176-A; *Rotaru*, cited above, § 57-59; *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-...; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 75-77, 28 June 2007; *Liberty and Others v. the United Kingdom*, no. 58243/00, § 62-63, 1 July 2008). The Court notes, however, that these questions are in this case closely related to the broader issue of whether the interference was necessary in a democratic society. In view of its analysis in paragraphs 105-126 below, the Court does not find it necessary to decide whether the wording of section 64 meets the "quality of law" requirements within the meaning of Article 8 § 2 of the Convention.

(b) Legitimate aim

100. The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection, and therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders.

(c) Necessary in a democratic society

(i) General principles

101. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention (see *Coster v. the United Kingdom* [GC], no. 24876/94, § 104, 18 January 2001, with further references).

102. A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see *Connors v. the United Kingdom*, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007-...). Where, however, there is no consensus within the Member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see *Dickson v. the United Kingdom* [GC], no. 44362/04, § 78, ECHR 2007-...).

103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, *mutatis mutandis*, *Z.*, cited above, § 95). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned,

not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and 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 (see Article 5 of the Data Protection Convention and the preamble thereto and Principle 7 of Recommendation R(87)15 of the Committee of Ministers regulating the use of personal data in the police sector). The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention). The above considerations are especially valid as regards the protection of special categories of more sensitive data (see Article 6 of the Data Protection Convention) and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family (see Recommendation No. R(92)1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system).

104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned (see, *mutatis mutandis*, *Z.* cited above, § 96).

(ii) Application of these principles to the present case

105. The Court finds it to be beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification. The techniques of DNA analysis were acknowledged by the Council of Europe more than fifteen years ago as offering advantages to the criminal-justice system (see Recommendation R(92)1 of the Committee of Ministers, paragraphs 43-44 above). Nor is it disputed that the member States have since that time made rapid and marked progress in using DNA information in the determination of innocence or guilt.

106. However, while it recognises the importance of such information in the detection of crime, the Court must delimit the scope of its examination. The question is not whether the retention of fingerprints, cellular samples and DNA profiles may in general be regarded as justified under the Convention. The only issue to be considered by the Court is whether the retention of the fingerprint and DNA data of the applicants, as persons who

had been suspected, but not convicted, of certain criminal offences, was justified under Article 8, paragraph 2 of the Convention.

107. The Court will consider this issue with due regard to the relevant instruments of the Council of Europe and the law and practice of the other Contracting States. The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (see paragraphs 41-44 above). These principles appear to have been consistently applied by the Contracting States in the police sector in accordance with the Data Protection Convention and subsequent Recommendations of the Committee of Ministers (see paragraphs 45-49 above).

108. As regards, more particularly, cellular samples, most of the Contracting States allow these materials to be taken in criminal proceedings only from individuals suspected of having committed offences of a certain minimum gravity. In the great majority of the Contracting States with functioning DNA databases, samples and DNA profiles derived from those samples are required to be removed or destroyed either immediately or within a certain limited time after acquittal or discharge. A restricted number of exceptions to this principle are allowed by some Contracting States (see paragraphs 47-48 above).

109. The current position of Scotland, as a part of the United Kingdom itself, is of particular significance in this regard. As noted above (see paragraph 36), the Scottish Parliament voted to allow retention of the DNA of unconvicted persons only in the case of adults charged with violent or sexual offences and even then, for three years only, with the possibility of an extension to keep the DNA sample and data for a further two years with the consent of a sheriff.

110. This position is notably consistent with Committee of Ministers' Recommendation R(92)1, which stresses the need for an approach which discriminates between different kinds of cases and for the application of strictly defined storage periods for data, even in more serious cases (see paragraphs 43-44 above). Against this background, England, Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence.

111. The Government lay emphasis on the fact that the United Kingdom is in the vanguard of the development of the use of DNA samples in the detection of crime and that other States have not yet achieved the same maturity in terms of the size and resources of DNA databases. It is argued that the comparative analysis of the law and practice in other States with less advanced systems is accordingly of limited importance.

112. The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of

such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.

113. In the present case, the applicants' fingerprints and cellular samples were taken and DNA profiles obtained in the context of criminal proceedings brought on suspicion of attempted robbery in the case of the first applicant and harassment of his partner in the case of the second applicant. The data were retained on the basis of legislation allowing for their indefinite retention, despite the acquittal of the former and the discontinuance of the criminal proceedings against the latter.

114. The Court must consider whether the permanent retention of fingerprint and DNA data of all suspected but unconvicted people is based on relevant and sufficient reasons.

115. Although the power to retain fingerprints, cellular samples and DNA profiles of unconvicted persons has only existed in England and Wales since 2001, the Government argue that their retention has been shown to be indispensable in the fight against crime. Certainly, the statistical and other evidence, which was before the House of Lords and is included in the material supplied by the Government (see paragraph 92 above) appears impressive, indicating that DNA profiles that would have been previously destroyed were linked with crime-scene stains in a high number of cases.

116. The applicants, however, assert that the statistics are misleading, a view supported in the Nuffield Report. It is true, as pointed out by the applicants, that the figures do not reveal the extent to which this "link" with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons. Nor do they demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons. At the same time, in the majority of the specific cases quoted by the Government (see paragraph 93 above), the DNA records taken from the suspects produced successful matches only with earlier crime-scene stains retained on the data base. Yet such matches could have been made even in the absence of the present

scheme, which permits the indefinite retention of DNA records of all suspected but unconvicted persons.

117. While neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position, the Court accepts that the extension of the database has nonetheless contributed to the detection and prevention of crime.

118. The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed (see paragraph 35 above); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

120. The Court acknowledges that the level of interference with the applicants' right to private life may be different for each of the three different categories of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue calls for careful scrutiny regardless of these differences.

121. The Government contend that the retention could not be considered as having any direct or significant effect on the applicants unless matches in the database were to implicate them in the commission of offences on a future occasion. The Court is unable to accept this argument and reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data (see paragraph 67 above).

122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the

applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal (see *Asan Rushiti v. Austria*, no. 28389/95, § 31, 21 March 2000, with further references). It is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed.

123. The Government argue that the power of retention applies to all fingerprints and samples taken from a person in connection with the investigation of an offence and does not depend on innocence or guilt. It is further submitted that the fingerprints and samples have been lawfully taken and that their retention is not related to the fact that they were originally suspected of committing a crime, the sole reason for their retention being to increase the size and, therefore, the use of the database in the identification of offenders in the future. The Court, however, finds this argument difficult to reconcile with the obligation imposed by section 64(3) of the PACE to destroy the fingerprints and samples of volunteers at their request, despite the similar value of the material in increasing the size and utility of the database. Weighty reasons would have to be put forward by the Government before the Court could regard as justified such a difference in treatment of the applicants' private data compared to that of other unconvicted people.

124. The Court further considers that the retention of the unconvicted persons' data may be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society. The Court has already emphasised, drawing on the provisions of Article 40 of the UN Convention on the Rights of the Child of 1989, the special position of minors in the criminal-justice sphere and has noted in particular the need for the protection of their privacy at criminal trials (see *T. v. the United Kingdom* [GC], no. 24724/94, §§ 75 and 85, 16 December 1999). In the same way, the Court considers that particular attention should be paid to the protection of juveniles from any detriment that may result from the retention by the authorities of their private data following acquittals of a criminal offence. The Court shares the view of the Nuffield Council as to the impact on young persons of the indefinite retention of their DNA material and notes the Council's concerns that the policies applied have led to the over-representation in the database of young persons and ethnic minorities, who have not been convicted of any crime (see paragraphs 38-40 above).

125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

126. Accordingly, there has been a violation of Article 8 of the Convention in the present case.

II. ALLEGED VIOLATION OF ARTICLE 14 TAKEN TOGETHER WITH ARTICLE 8 OF THE CONVENTION

127. The applicants submitted that they had been subjected to discriminatory treatment as compared to others in an analogous situation, namely other unconvicted persons whose samples had still to be destroyed under the legislation. This treatment related to their status and fell within the ambit of Article 14, which had always been liberally interpreted. For the reasons set out in their submissions under Article 8, there was no reasonable or objective justification for the treatment, nor any legitimate aim or reasonable relationship of proportionality to the purported aim of crime prevention, in particular as regards the samples which played no role in crime detection or prevention. It was an entirely improper and prejudicial differentiation to retain materials of persons who should be presumed to be innocent.

128. The Government submitted that as Article 8 was not engaged Article 14 of the Convention was not applicable. Even if it were, there was no difference of treatment as all those in an analogous situation to the applicants were treated the same and the applicants could not compare themselves with those who had not had samples taken by the police or those who consented to give samples voluntarily. In any event, any difference in treatment complained of was not based on “status” or a personal characteristic but on historical fact. If there was any difference in treatment, it was objectively justified and within the State's margin of appreciation.

129. The Court refers to its conclusion above that the retention of the applicants' fingerprints, cellular samples and DNA profiles was in violation of Article 8 of the Convention. In the light of the reasoning that has led to

this conclusion, the Court considers that it is not necessary to examine separately the applicants' complaint under Article 14 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

130. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

131. The applicants requested the Court to award them just satisfaction for non-pecuniary damage and for costs and expenses.

A. Non-pecuniary damage

132. The applicants claimed compensation for non-pecuniary damage in the sum of GBP 5,000 each for distress and anxiety caused by the knowledge that intimate information about each of them had been unjustifiably retained by the State, and in relation to anxiety and stress caused by the need to pursue this matter through the courts.

133. The Government, referring to the Court's case-law (in particular, *Amann v. Switzerland*, cited above), submitted that a finding of a violation would in itself constitute just satisfaction for both applicants and distinguished the present case from those cases where violations had been found as a result of the use or disclosure of the personal information (in particular, *Rotaru v. Romania*, cited above).

134. The Court recalls that it has found that the retention of the applicants' fingerprint and DNA data violates their rights under Article 8. In accordance with Article 46 of the Convention, it will be for the respondent State to implement, under the supervision of the Committee of Ministers, appropriate general and/or individual measures to fulfil its obligations to secure the right of the applicants and other persons in their position to respect for their private life (see *Scozzari and Giunta v. Italy* [GC], nos. 39221/98 and 41963/98, § 249, ECHR 2000-VIII, and *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 120, ECHR 2002-VI). In these circumstances, the Court considers that the finding of a violation, with the consequences which will ensue for the future, may be regarded as constituting sufficient just satisfaction in this respect. The Court accordingly rejects the applicants' claim for non-pecuniary damage.

B. Costs and expenses

135. The applicants also requested the Court to award GBP 52,066.25 for costs and expenses incurred before the Court and attached detailed documentation in support of their claim. These included the costs of the solicitor (GBP 15,083.12) and the fees of three counsel (GBP 21,267.50, GBP 2,937.50 and GBP 12,778.13 respectively). The hourly rates charged by the lawyers were as follows: GBP 140 in respect of the applicants' solicitor (increased to GBP 183 as from June 2007) and GBP 150, GBP 250 and GBP 125 respectively in respect of the three counsel.

136. The Government qualified the applicants' claim as entirely unreasonable. They submitted in particular that the rates charged by the lawyers were excessive and should be reduced to no more than two-thirds of the level claimed. They also argued that no award should be made in respect of the applicants' decision to instruct a fourth lawyer at a late stage of the proceedings as it had led to the duplication of work. The Government concluded that any cost award should be limited to GBP 15,000 and in any event, to no more than GBP 20,000.

137. The Court reiterates that only legal costs and expenses found to have been actually and necessarily incurred and which are reasonable as to quantum are recoverable under Article 41 of the Convention (see, among other authorities, *Roche v. the United Kingdom* [GC], no. 32555/96, § 182, ECHR 2005-X).

138. On the one hand, the present applications were of some complexity as they required examination in a Chamber and in the Grand Chamber, including several rounds of observations and an oral hearing. The application also raised important legal issues and questions of principle requiring a large amount of work. It notably required an in-depth examination of the current debate on the issue of retention of fingerprint and DNA records in the United Kingdom and a comprehensive comparative research of the law and practice of other Contracting States and of the relevant texts and documents of the Council of Europe.

139. On the other hand, the Court considers that the overall sum of GBP 52,066.25 claimed by the applicants is excessive as to quantum. In particular, the Court agrees with the Government that the appointment of the fourth lawyer in the later stages of the proceedings may have led to a certain amount of duplication of work.

140. Making its assessment on an equitable basis and in the light of its practice in comparable cases, the Court awards the sum of EUR 42,000 in respect of costs and expenses, less the amount of EUR 2,613.07 already paid by the Council of Europe in legal aid.

C. Default interest

141. The Court considers it appropriate that the default interest should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Holds* that there has been a violation of Article 8 of the Convention;

2. *Holds* that it is not necessary to examine separately the complaint under Article 14 of the Convention;

3. *Holds* that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicants;

4. *Holds*
   (a) that the respondent State is to pay the applicants, within three months, EUR 42,000 (forty two thousand euros) in respect of costs and expenses (inclusive of any VAT which may be chargeable to the applicants), to be converted into pounds sterling at the rate applicable at the date of settlement, less EUR 2,613.07 already paid to the applicants in respect of legal aid;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicants' claim for just satisfaction.

Done in English and in French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 4 December 2008.

Michael O'Boyle	Jean-Paul Costa
Deputy Registrar	President