EVIDENCE TO THE JOINT COMMITTEE ON HUMAN RIGHTS CONCERNING THE PROVISIONS OF THE POLICING AND CRIME BILL THAT RELATE TO THE USE AND RETENTION OF DNA PERSONAL DATA AND CCTV/ANPR IMAGES

Dr C. N. M. Pounder[1]
www.amberhawk.com
(March 2009)

This evidence is limited to commentary on New Clause 33 (NC33) which provides for wide ranging powers in relation to the use and retention of personal data, in particular CCTV and Automated Number Plate Readers (ANPR) images, and personal data derived from DNA samples. The Government has explained that the clause is its response following the loss of its ECHR case in *S and Marper v The United Kingdom*[2] . NC33 was inserted into the Policing and Crime Bill at the end of its Commons Committee stage; its function is to insert new section 64B into the Police & Criminal Evidence (PACE) Act 1984. For convenience, it is reproduced in the Appendix.

In outline, the Government is seeking to acquire extensive powers to use and retain personal data in sensitive areas, and this acquisition is likely to significantly reduce the protection afforded by the Data Protection Act. The provisions have been introduced in advance of a promised public consultation on DNA retention; there never has been a public consultation over the use of CCTV or ANPR images. The fact that secondary legislation is used in these areas ensures that there is limited Parliamentary scrutiny over the detail of Government proposals.

The evidence makes five recommendations that help remedy these failings.

1. THE FIVE RECOMMENDATIONS (A-E)

A. . There should be no need to remind the Committee of the number of times it has made comments about its inability to scrutinise such wide-ranging statutory powers which impact on Article 8 ECHR, nor to refer to the omission of a human rights memorandum

[1] *I have been working in data protection for more than twenty years and have given oral or written evidence to several Committees of both Houses of Parliament, including previous written evidence to the JCHR. All the historic evidence I have provided to the House is accessible from* ***www.amberhawk.com***.

[2] *S. and Marper v. The United Kingdom - 30562/04 [2008] ECHR 1581* (*4 December 2008)*

which would explain why the exercise of these new powers is likely to be consistent with human rights legislation[3]. Once again, these very issues are presented in a heightened way in relation to the DNA database and in connection with the most widely used surveillance cameras in the UK.

Consequently, without providing the detail, I repeat my recommendations made in my written evidence to the Committee concerning similar extensive powers associated with the content of Information Sharing Orders as described in the Coroners and Justice Bill[4].

I recommend:

i. **A linkage between Article 8 ECHR and Data Protection Act via the Sixth Data Protection Principle (dealing with rights of data subjects); this will introduce a privacy right limited to the processing of personal data.**

ii. **A new power for the Information Commissioner to challenge an Order made under any legislation on the grounds that the Order requires the processing of personal data in a way inconsistent with Article 8.**

iii. **The independence of the Information Commissioner who becomes funded by Parliament and reports to a relevant Parliamentary Committee.**

iv. **An enhanced right to object to the processing of personal data in circumstances where the processing is not for a purpose identified in Article 8(2).** Note that this extended right to object is not designed to apply to that processing necessary for legitimate law enforcement.

B. New section 64B to the Police and Criminal Evidence Act 1984 begins:

> *"(1) The Secretary of State may by regulations make provision as to the retention, use and destruction of material to which this section applies."*

I recommend that the following subsection is added after subsection (1) in the new section 64B.

> *"(xx) Regulations made under subsection (1) shall not specify any measure that relates to the processing of personal data that is derived from material falling within subsections (2)(a) and (e) of this section".*

---

[3] *See the Joint Committee on Human Rights (JCHR), 6th Report, Session 2007-8; Joint Committee on Human Rights (JCHR), 8th Report, Session 2004-5; Joint Committee on Human Rights (JCHR), 12th Report, Session 2004-5; Joint Committee on Human Rights (JCHR), 14th Report, Session 2007-8 and Joint Committee on Human Rights (JCHR), 16th Report, Appendix 20D, Session 2006-7 and Joint Committee on Human Rights (JCHR), 19th Report, Session 2004-5. Recommendations 59 and 60 of the Home Affairs Select Committee's report into ID Cards (session 2004/5); described powers in the ID Card Bill as "unacceptable", yet they exist in the ID Card Act 2006 in the same form.*

[4] *The complete analysis of Section 152 of the Coroners and Justice Bill is available on www.amberhawk.com*

Section 2 of this evidence provides background in support of this change. The argument in summary is as follows: if there are no powers for Ministers to apply in connection with the use or retention of personal data relating to DNA samples or photographs, then the balance of "police need for DNA or photographic personal data" versus the "protection of the individual" becomes subject to the Data Protection Act and its well established, independent regulatory framework.

C. The definition of "photograph to include a moving image" in section 64B(10) could provide a statutory basis for the retention or use of CCTV images as part of ACPO's National CCTV Strategy[5]. As recommendation 3.2 of ACPO's National CCTV Strategy suggested that primary legislation was needed to cover a number of deficiencies covering the legislation relevant to CCTV surveillance, there is a risk that this definition could legitimise that strategy by means of secondary legislation in contradiction to ACPO's recommendation (and with minimal Parliamentary scrutiny).

The definition is discussed in section 3 of this evidence as it also covers images collected by ANPR systems[6]. These images too have not been subject to public debate, Parliamentary scrutiny and both the Surveillance Commissioner and Information Commissioner have both expressed concern over ANPR systems.

I have found no evidence that the Government has, in relation to new section 64B, considered any of the recommendations of the two Parliamentary Committees that have considered the Surveillance Society[7]. In addition, I am not aware of any Privacy Impact Assessments that have been published by Government re ANPR/DNA/CCTV.

As it is difficult to foretell the future of technological developments that relate to DNA and CCTV/ANPR, **I recommend that the Committee insert a "sunset clause" into section 64B which is activated in 2015.** This sunset clause will ensure that a future Parliament can revisit this subject in a few years time and take an informed view of the implications of giving Ministers wide ranging powers to determine of "use" and "retention" of DNA and CCTV/ANPR images in the light of technological advancements.

---

[5] *http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.htm*

[6] *See for example, "Britain will be first country to monitor every car journey" http://www.independent.co.uk/news/uk/home-news/britain-will-be-first-country-to-monitor-every-car-journey-520398.html*

[7] "*Surveillance: Citizens and the State" (House of Lords Constitution Committee; HL 18, Session 2008-09) and "A Surveillance Society" (House of Commons Home Affairs Committee; HC 58, Session 2007-08*)

D. I repeat the observation I made to Marper's legal team when I prepared a data protection analysis for them[8]. Because of the genetic linkages between the generations of family members, the Home Office's DNA database (if unchecked) possesses the potential to span most of the population of the UK. The analysis in the section 4 to this evidence shows that this possibility arises from the combination of the view of the European Court of Human Rights that the retention of DNA relating to offenders does not breach Article 8[9], and the assumption that familial DNA techniques will become more commonplace.

E. I recommend the Committee firmly reject the weak regulatory system established by provisions in Section 64B as lacking independence and credibility.

This weak system of regulation arises because the Home Secretary controls the functions and reporting structure of the regulator, has jurisdiction over what is regulated, and is also politically responsible for the public bodies that are subject to regulation. The Committee should recognise the inherent conflict of interest when, for example, the Home Secretary sets public policy in relation to DNA samples or CCTV/ANPR surveillance **and** also provides for privacy protection in these areas.

Note that my **Recommendation A** would ensure that the Information Commissioner could challenge Orders which were in breach of Article 8. **Recommendation B** would ensure that the processing of personal data would be subject to regulation by the Data Protection Act and allow the Commissioner to establish the degree of independent regulation. **Recommendation C** would allow a future Parliament to review these matters in 2015.

The Committee should unambiguously state that the Home Secretary's powers over the regulator are unacceptable. The provisions in Section 64B propose a situation that is akin to that which would arise if Count Dracula were given the responsibility for policy at the National Blood Transfusion Service and was seeking powers to appoint his own auditors to make recommendations as to the distribution, quantity and quality of the blood supply**.**

The same argument applies to any regulator appointed in relation to CCTV and ANPR.

---

[8] *This analysis is also available on www.amberhawk.com*

[9] *Decision as to the Admissibility of Application 29514/05, Hendrick Jan Van der Velden against the Netherlands*

2. MAIN CONCLUSIONS OF A DATA PROTECTION ANALYSIS

(a) The position established by Section 64B

New Section 64B(2) of PACE allows Ministers to enact regulations that to relate to:

> "(a) photographs falling within a description specified in the regulations,
>
> (b) fingerprints taken from a person in connection with the investigation of an offence,
>
> (c) impressions of footwear so taken from a person,
>
> (d) DNA and other samples so taken from a person,
>
> (e) information derived from DNA samples so taken from a person".

It is noteworthy that this subsection has two paragraphs in relation to DNA and only one in relation to fingerprints. One would conclude, therefore, that if fingerprints were destroyed, personal data relating to those fingerprints would also be destroyed. However, this is not the case with DNA. If the DNA sample were destroyed, the power in paragraph (e) could ensure that the related DNA personal data could be retained for longer periods (e.g. indefinitely) or used for something else (e.g. for a research purpose or any other purpose).

When the Government's amendment was promoted in Committee[10], the Minister made no statement as to why there were two provisions with respect to DNA – nor was there any comment in relation to CCTV/ANPR. Yet these provisions are so flexible that they could allow Ministers to lawfully retain and use DNA personal data in circumstances which, without those regulations to provide the statutory basis, could be in breach of several data protection principles. The same position pertains to CCTV/ANPR images.

(b) The position if Recommendation B is accepted

Recommendation B requires the following subsection to be included in Section 64B.

> *"(xx) Regulations made under subsection (1) shall not specify any measure that relates to the processing of personal data that is derived from material falling within subsections (2)(a) and (e)".*

The effect of this change is to leave any matter that relates to the processing of personal data to the Data Protection Act. This means that the retention periods are not established by Ministerial *fiat* in regulations; they are established by a mechanism that balances the interests of the police versus the interests of the policed and regulated by the Information Commissioner. This

[10] *http://www.publications.parliament.uk/pa/cm200809/cmpublic/policing/090226/pm/90226s06.htm*

provides a system of independent checks and balances, and appeals to the judicial system in cases of dispute.

For example, the Data Protection Act would not preclude the processing of a DNA personal data derived from a sample taken from somebody arrested and using those data in relation to any inquiry. The Act would not prevent DNA personal data derived from a sample being processed and comparisons been made with samples found at the scene of a crime or other scenes of crime. The Act would not require DNA personal data to be deleted by the police, if such data could be justified in terms of retention with respect to ongoing inquiries or likely inquiries. All processing of DNA personal data that were necessary for the statutory functions of the police, that were relevant for a policing purpose, that were needed to be retained or used for a policing purpose, could all be lawfully processed.

However, a data protection analysis would arrive at a range of different retention periods for the DNA personal data that define the circumstances when they were no longer needed for a policing purpose. This retention time would depend on a number of factors such as the status of the data subject (convicted, arrested), the likelihood of recidivism, the age of the data subject, the length of time which had passed since the data subject last came to police attention, and the seriousness of the crime involved or being investigated. These are the very items that have been identified by the Government in its public pronouncements on the retention of DNA[11].

The need for a variety of retention criteria is manifestly apparent from published criminal statistics. For example[12], criminal statistics relating to those born between 1953 and 1978 reveal that "the majority of offenders had been convicted on only one occasion" and that "the peak age of known criminal activity for males was nineteen". If this is the case, data protection could require consideration of the deletion of DNA personal data if (a) the offence was minor; (b) the offender had not repeated a crime; (c) the offender was of a certain maturity (e.g. over 30), and (d) that the police had no interest in the data subject for some years.

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

(a) those identified individuals who are convicted of minor offences.
(b) those identified individuals who are convicted of serious offences.
(c) Juveniles who are processed by the criminal justice system

[11] *The speech of the Home Secretary at the Intellect Technology Association (16th December 2008) http://press.homeoffice.gov.uk/press-releases/common-sense-standards.*

[12] *http://www.homeoffice.gov.uk/rds/pdfs/hosb401.pdf*

(d) those identified individuals who are arrested and whose DNA matches that found at another scene of crime.

(e) those identified individuals who are arrested but are not convicted or proceeded against.

(f) those identified individuals whose samples need to be eliminated from the DNA found at the scene of crime.

(g) those unidentified individuals whose DNA is found at the scene of a crime.

(h) those who help the police and consent to the DNA personal data being processed

(i) those who are involved or suspects in offences of a sexual nature.

It can be seen that DNA personal data in category (b), (g) and (i) are likely to be kept indefinitely whereas (h) would be retained until consent is withdrawn; some special retention rules might apply for category (c) and the retention times for (a) would be longer that (e).

However, this granular approach would be jeopardized if any future Ministers can specify retention periods independently of the Data Protection Act. If, for example, a Minister for stipulated in an Order that DNA personal data can be retained for 20 years, that time period would become the lawful retention period – irrespective of any data protection analysis that may point to a shorter retention period as being more appropriate.

It should be added that the same argument is equally pressing in relation to the processing of CCTV/ANPR photographic images by the police. Like the powers in the Coroners and Justice Bill, these powers in NC33 are so wide that the Home Secretary could determine excessive retention periods and uses that were incompatible with a policing purpose (See section 4).

It seems very curious that Home Secretary in December 2008 wanted to "enjoy the confidence and trust of the public" in the DNA database and proposed that changes will be set out in the White Paper that in order to "deliver a more proportionate, fair and common sense approach"[13]. Yet, in advance of that public consultation, this Bill provides a framework for the lawful use and retention of DNA and related personal data. If there is to be a meaningful public debate over DNA retention, why is there a need to determine the relevant legal framework in advance? Perhaps clairvoyant civil servants and Ministers already know the conclusions of that debate.

My own view is that specific primary legislation should be enacted when Government has finalised its plans, delivered on its promised public consultation, and reported to the European Court of Human Rights on its course of action. In many privacy matters that require a balancing act to be performed, the devil is in the detail of actual processing procedures. Such detail is not

[13] *Part of her speech to Intellect Technology Association (reference 11)*

going to be debated or scrutinised via a procedure that provides for wide ranging powers, which gain little scrutiny in Parliament**. I hope the Committee will support that view.**

3. "PHOTOGRAPHS OF A MOVING IMAGE"

New Section 64B(10) of PACE reads as follows: "(10) For the purposes of this section—(a) 'photograph' includes a moving image....".

The most obvious photographic "moving image" relates to those images captured by CCTV and ANPR surveillance. This means that the wide ranging Ministerial powers in the Section 64B are engaged in connection with the use and retention of CCTV/ANPR images. The Minister in moving the the clause in Committee, for some reason, did not make any comment in relation to the surveillance connection[14].

ACPO's National CCTV Strategy[15] sets out plans for co-ordinating an ambitious, integrated expansion of the CCTV in town centres to include "CCTV from buses, tube and train carriages" and from "football stadiums, arenas and other areas of public convenience". The Strategy foresees other electronic linkages for localised CCTV systems such as in a store or railway station: these include "shop cameras to Electronic Point of Sale systems", "transport system cameras to travel cards" and "internal building cameras connected to building access control systems". Such integration, the Strategy states, will "dramatically improve the effectiveness of CCTV systems" as "post event CCTV images can quickly be searched against other events".

One important reason for these linkages is that, in the post 9/11 world, the Strategy is subtly enhancing the role of CCTV from its accepted role that relates to crowds in city centres (e.g. public safety, public order or low-level street-crime) to ensure that such CCTV, in future, has the functionality to trace individuals and vehicles involved in serious crime and for anti-terrorist purposes. The Strategy clearly states that "if we are to deal more effectively with serious, organized crime and terrorism, different operational requirements are needed".

As is widely known, London's Congestion Charge ANPR cameras now feed images through to MI5 for national security purposes, and modern digital CCTV in city centres are increasingly augmented by ANPR functionality that permits checks with the Police National Computer (e.g. to

---

[14] *http://www.publications.parliament.uk/pa/cm200809/cmpublic/policing/090226/pm/90226s06.htm*

[15] *See reference 5*

provide intelligence on vehicle movements, to identify uninsured drivers). The Strategy envisages that CCTV will develop facial recognition functionality in future, and one can see such systems being used in relation to ASBOs or surveillance of individuals of interest to the police. In this way, the police's use of CCTV, linked to ANPR, to support its policy of "Denying Criminals the Use of the Road[16]" could possibly develop into a policy of "Denying Criminals the Use of the Pavement".

The Committee should raise serious objection to ANPR/CCTV images being legitimised by the exercise of wide ranging powers and subject to minimal scrutiny and no public debate. This was one main mistake made with DNA sample collection and related database – no public debate, little Parliamentary scrutiny, and lengthy and expensive Court proceedings. **That is why the Committee could support Recommendations A, B & C.** (CCTV/ANPR should be regulated by the Data Protection Act, there should be an ability to challenged orders that could breach Article 8 and a sunset clause should be included in section 64B).

Finally, in this section, it appears to be a little disingenuous to promote a New Clause with a claim that its objective is to resolve a serious breach of Article 8 re DNA, and slip in, without any announcement, a subtle definitional change that extends surveillance via the use and retention of ANPR and CCTV images. I think this kind of "double dealing" can only undermine public trust in the political process.

4. WHY THE DNA DATABASE MAY SPAN THE POPULATION

DNA testing kits are often marketed with statements such as "confirm with 100% accuracy if a child is related to their Grandparent". If this claim is true, it means the DNA of child maps through its parents to the "parents of the parents" or Grandparents (or at least 5 individuals)[17]. The UK has a population of 60,000,000. As there are very high statistically significant links of one DNA profile to say 4-6 close members of a family (e.g. between parents, grandparents and siblings), then each entry in the DNA database can be considered as having the potential to span at least 5 other family members.

The ECHR has already accepted in the case of Van der Velden[18], that because of his offences, his Article 8 rights were not infringed by the retention of his DNA and any related personal data;

---

[16] *http://police.homeoffice.gov.uk/publications/operational-policing/ANPR_10,000_Arrests.pdf?view=Standard&pubID=288680*

[17] *For example, the grandparent test on http://www.dna-worldwide.com/relationship-testing/grand-parent-test*

[18] *See Van Velden, reference 9*

this means that the interference arising from retaining DNA personal data in relation to offenders has a lawful basis.

The current size of the DNA database has 3-4 million entries relating to offenders; the use of familial linkages implies that the database has the potential to span about 15-25 million individuals or between 20%-40% of the population, many of whom will not be offenders. It follows that a database of 10-12 million offenders clearly has the potential span the vast majority of the UK population. In other words, the mathematics of family genetics means that a DNA database of this potential is probably only few technical innovations away.

It is recognised that this prospect is not a realistic one given the state of today's technology or current DNA practice. However, if following Marper, the police cannot use DNA samples of the "innocent", then one would expect scientific and statistical techniques to be developed that exploit the genetic links between offenders and their family members. As techniques improve, they become cheaper and it is to be expected that familial line DNA analysis can become more effective, possibly extended to the more remote family members. The reason why the police keep DNA samples beyond the death of the person from whom the sample was taken is, in part, a tacit recognition that the DNA sample can relate to other individuals and that such techniques could improve familial tracing[19].

Criminal statistics regularly show that, approximately, about one third of males and one-tenth of women have a criminal record other than motoring offences[20]. Assume these level remain constant, and assume that DNA continues to taken from those convicted, the maximum DNA database coverage of the population will inevitably approach 20-25% (assuming DNA is taken from those men and women who commit a criminal offences).

Such a national DNA database of the future (if unchecked) thus has the potential to span 80%-100% of the population – the only question is **when this coverage will occur**. That is why I have made recommendations B & C (the use and retention of DNA personal data should be regulated by the Data Protection Act, and a "sunset" clause should be included in Section 64B so that Parliament can re-evaluate this database).

Dr. C. N. M. Pounder
www.amberhawk.com
March 2009

---

[19] *ACPO DNA Good Practice Manual, Second Edition 2005,Appendix 1*

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

APPENDIX 1: NEW CLAUSE 33

Retention and destruction of samples etc: England and Wales

'(1) After section 64A of the Police and Criminal Evidence Act 1984 (c. 60) insert—

"64B Retention and destruction of samples etc

(1) The Secretary of State may by regulations make provision as to the retention, use and destruction of material to which this section applies.

(2) This section applies to the following material—

(a) photographs falling within a description specified in the regulations,

(b) fingerprints taken from a person in connection with the investigation of an offence,

(c) impressions of footwear so taken from a person,

(d) DNA and other samples so taken from a person,

(e) information derived from DNA samples so taken from a person.

(3) The regulations may—

(a) make different provision for different cases, and

(b) make provision subject to such exceptions as the Secretary of State thinks fit.

(4) The regulations may frame any provision or exception by reference to an approval or consent given in accordance with the regulations.

(5) The regulations may confer functions on persons specified or described in the regulations.

(6) The functions which may be conferred by virtue of subsection (5) include those of—

(a) providing information about the operation of regulations made under this section,

(b) keeping their operation under review,

(c) making reports to the Secretary of State about their operation, and

(d) making recommendations to the Secretary of State about the retention, use and destruction of material to which this section applies.

(7) The regulations may make provision for and in connection with establishing a body to discharge the functions mentioned in subsection (6)(b) to (d).

(8) The regulations may make provision amending, repealing, revoking or otherwise modifying any provision made by or under an Act (including this Act).

(9) The provision which may be made by virtue of subsection (8) includes amending or otherwise modifying any provision so as to impose a duty or confer a power to make an order, regulations, a code of practice or any other instrument.

(10) For the purposes of this section—

(a) "photograph" includes a moving image, and

(b) the reference to a DNA sample is a reference to any material that has come from a human body and consists of or includes human cells.

64C Retention and destruction of samples etc: supplementary

(1) Regulations under section 64B may make—

(a) supplementary, incidental or consequential provision, or

(b) transitional, transitory or saving provision.

(2) Regulations under that section are to be made by statutory instrument.

(3) An instrument containing regulations under that section may not be made unless a draft of the instrument has been laid before, and approved by resolution of, each House of Parliament."

(2) The amendment made by subsection (1) applies in relation to material obtained before or after the commencement of this section.'.—*(Mr. Campbell.)*

This amendment, responding to the ECtHR judgement in S and Marper v UK on 4 December 2008, would amend the Police and Criminal Evidence Act 1984, creating a power to make regulations on the retention, use and destruction of photographs, fingerprints, footwear impressions, DNA and other samples and DNA profiles.
Brought up, and read the First time.