THE PROVISIONS OF THE CRIME AND SECURITY BILL THAT RELATE TO THE RETENTION OF PERSONAL DATA ON THE DNA DATABASE

(EVIDENCE TO THE JOINT COMMITTEE ON HUMAN RIGHTS)

AMBERHAWK

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, JANUARY 2010

THE PROVISIONS OF THE CRIME AND SECURITY BILL THAT RELATE TO THE RETENTION OF PERSONAL DATA ON THE DNA DATABASE

SUMMARY

The recommendations I would like the Committee to consider are:

a. **The definition of "recordable offences" in PACE should be subject to affirmative resolution procedures rather than negative resolution procedures. The Committee should take the opportunity to call for a document that reviews all negative resolution powers in the context of the processing of personal data by all law enforcement agencies**

b. **The Information Commissioner is, by default, the main regulator with respect to personal data stored on the DNA database. The Government should explain why the natural balance achieved by Data Protection Act (between the interests of the police DNA personal data retention and the interests of the data subjects in having DNA deleted), has been tipped in favour of retention (especially in the light of recommendation (f) below).**

c. **If DNA data on the dead are to be retained indefinitely on the database, then the Information Commissioner should have powers over these data as if they were personal data.**

d. **The DNA database associated with Crime and Security Bill should be the only DNA database established by the law enforcement agencies. If records from DNA database can be copied by the national security agencies for their purposes, then the minimal protective measures in the Bill are undermined.**

e. **The Human Genetics Commissioner should be asked whether all DNA databases containing personal data should be identified with the long term aim of bringing them under specific DNA related legislation approved by Parliament.**

f. **The Government's statistical analysis does not withstand close analysis; even the evidence for indefinite retention of DNA on criminals is suspect. Indefinite retention linked to familial DNA techniques is likely to eventually result in a universal DNA database. The precautionary principle should therefore be applied and the Bill should be amended to**

include a "sunset" clause so that it is subject to Parliamentary re-approval every seven years. This would allow Parliament to reassess the DNA provisions in the Bill in the light of technical advances.

I cannot be the only one who has found analysis of this Bill difficult. Its expression as amendments to the Police and Criminal Evidence Act (PACE) 1984, itself heavily amended by several Acts of Parliament, means that the public cannot see clearly how the Bill works in practice[1], especially in the context of the powers in PACE and in other Acts of Parliament. The Committee might want to comment on the particular lack of accessibility of this Bill.

1. Justification for recommendation (a)

Recommendation (a): *The definition of "recordable offences" in PACE should be subject to affirmative resolution procedures rather than negative resolution. The Committee should take the opportunity to call for a document that reviews all negative resolution powers in the context of the processing of personal data by all law enforcement agencies.*

Summary of argument: *The Government's proposals allow the police to retain a DNA sample and related personal data if the offence is a "recordable offence". The expansive meaning of a "recordable offence" in the Police and Criminal Evidence Act is subject to minimal Parliamentary scrutiny (negative resolution). This negates the impact of affirmative resolution procedures in the Bill.*

The Government has included in the Bill an amendment to repeal Sections 27(1) to 27(3) of PACE[2]. It is surprising that Home Office, having examined Section 27 of PACE, concluded that Sections 27(4) & 27(5) did not need changing – as is explained below.

Sections 27(4&5) of the Police and Criminal Evidence Act 1984 states that "The Secretary of State may by regulations make provision for recording in national police records convictions for such offences as are specified in the regulations" where "regulations under this section shall be made by statutory instrument and shall be subject to annulment in pursuance of a resolution of either House of Parliament".

In 2000, when the National Police Records (Recordable Offences) Regulations were enacted there was no Parliamentary debate[3] (see reference below) cautions, reprimands and warnings

---

[1] *The Statute Law database organised by the Ministry of Justice in relation to PACE carries the warning that "**Update Status Warning:** There are effects on this legislation that have not yet been applied to the Statute Law Database for the following year(s): 2009". This does not help the public to examine the effect of the Bill.*

[2] *See page 14 of the Bill at line 3 (Part of clause 6 of the Bill that introduces Schedule 2A into the PACE – the reference relates to paragraph 17 of that Schedule (which appears to have no paragraph labelled (2))*

became "recordable offences". Subsequent to these regulations, individuals arrested in relation to these minor matters had their DNA sample retained indefinitely. A future Government wanting to expand the DNA database, could determine that motoring offences should be recordable.

I hope the Committee will say that it is unacceptable to extend the reach of the DNA database by negative resolution procedures. That is why the Committee should take the opportunity to call for a document that reviews all negative resolution powers in the context of the processing of personal data by all law enforcement agencies to assess whether Parliamentary scrutiny could be improved.

The Committee should note that the negative affirmation procedures in relation to "recordable offences" undermines the affirmative resolution procedures found in the Bill (for example, Clause 7(5), which introduces Article 63(3A)(3) and Article 63(3A)(4) (or line 10, page 15 of the Bill as published on First Reading).

2. Justification for recommendations (b) and (c)

Recommendation (b): *The Information Commissioner is, by default, the main regulator with respect to personal data stored on the DNA database. The Government should explain why the natural balance achieved by Data Protection Act (between the interests of the police DNA personal data retention and the interests of the data subjects in having DNA deleted), has been tipped in favour of retention (especially in the light of recommendation (f) below).*

Recommendation (c): *If DNA data on the dead are to be retained indefinitely on the database, then the Information Commissioner should have powers over these data as if they were personal data.*

Summary of argument: *The Government has decided not to have a specific "DNA Commissioner". This means that because DNA data are personal data, the Information Commissioner will become the prime regulator in relation to the Government's DNA retention provisions. However, the provisions in the Crime and Security Bill significantly diminish the Commissioner's powers to act as an independent regulator by minimising the impact of the Data Protection Principles. The Commissioner also has very limited remit in relation to DNA samples of those who are dead.*

Most of the entries in the DNA database are personal data subject to the Data Protection Act; the Act sets out Eight Data Protection Principles that provide a framework that balances the

[3] *The Joint Committee on Statutory Instruments Nineteenth Report stated in 2000 that there was nothing to report. (http://www.publications.parliament.uk/pa/jt199900/jtselect/jtstatin/47-xix/6503.htm)*

interests of the individual against the interests of the police (the data controller). The Bill disturbs this balance by defining the interests of the police in retention of DNA data as taking precedence. Arguably, this reflects the fact that there is a conflict of interest in that it is difficult for Home Secretary to establish a "fair" balance if he has political responsibility for the police and a vested interest in the outcome of any DNA retention policy.

If the issue of DNA retention were left to the Act, then the right to object and Fifth Principle (dealing with retention) would be engaged. This would allow a data subject, for example, to argue that although the police have processed the DNA data in accordance with its statutory needs, the processing has caused substantial unwarranted distress or substantial unwarranted damage. Note that this right to object balances the various interests, has an independent umpire (the Commissioner) and an accessible appeal process (The Tribunal) to determine whether or not DNA should be retained or not. Appeal to the Courts from the Tribunal is also possible. This framework does not need a data subject to take a Chief Constable to Court.

Instead, the Bill proposes that DNA personal data will be retained for specific periods of time (e.g. those convicted of a recordable offence have indefinite retention). This means that the Information Commissioner cannot enforce the Fifth Data Protection Principle dealing with retention, as the law has specified the lawful retention period. The right to object is also neutered because the retention is lawful. In summary, the Bill proposes the kind of "balance" that is achieved when Count Dracula decides whether patients or vampires should receive blood transfusions from the NHS.

Finally, the Commissioner cannot effectively regulate DNA data that relate to individuals who have died as personal data, by definition, have to relate to a living individual.

3. Justification for recommendations (d) and (e)

Recommendation (d): *The DNA database associated with Crime and Security Bill should be the only DNA database established by the law enforcement agencies. If records from DNA database can be copied by the national security agencies for their purposes, then the minimal protective measures in the Bill are undermined.*

Recommendation (e): *The Human Genetics Commissioner should be asked whether all DNA databases containing personal data should be identified with the long term aim of bringing them under specific DNA related legislation approved by Parliament.*

Summary of argument: *I have not found anything that prevents the national security agencies to maintain a separate copy of the DNA database. If this duplication were to be the case, then the Bill before Parliament affords little protection; hence the Committee should consider whether a provision in the Bill should ensure that only one national DNA database is established for all law enforcement and national security agencies.*

Recommendation (e) allows Parliament to take the first steps in deciding whether more general legislation with respect to DNA databases is needed. This is especially the case if existing wide ranging powers would permit lawful access by the law enforcement agencies to these other databases.

The Security Service Act 1996 changed the function of the national security agencies; it states that "it shall also be the function of the Service to act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime". It is reasonable to assume the Security Service and other national security agencies process personal data in relation to this objective.

This may mean that the national security agencies may keep copies of personal data that have been removed from the DNA database or indeed maintain a complete copy of the deleted items from the DNA database. Such a copy the DNA database appears not to be regulated by the Bill, yet DNA from such a database could be accessed by the police in relation to serious crime. This would undermine the effect of this Bill.

Consequently, for the avoidance of doubt, the Crime and Security Bill should specify that the DNA database mentioned in the Bill should the only one that can be established by the law enforcement and national security agencies.

Finally, I think that as a matter of principle, all DNA databases containing personal data should be regulated by Parliament. Recommendation (e) is the first step in assessing whether or not there is an issue for Parliament to resolve.

4. Justification for recommendation (f)

Recommendation (f): *The Government's statistical analysis does withstand close analysis; even the evidence for indefinite retention of DNA on criminals is suspect. Indefinite retention linked to familial DNA techniques is likely to eventually result in a universal DNA database. The precautionary principle should be applied and the Bill should be amended to include a "sunset" clause so that it is subject to Parliamentary re-approval every seven years. This would allow Parliament to reassess the Bill in the light of technical advances.*

Summary of argument:. *It can be shown that a 6 year retention period borders on the excessive in relation to the retention of DNA personal data in connection with those who have a criminal record. If public policy is to distinguish between criminals and non-criminals, it follows that six year retention is excessive in relation to the retention of DNA of non-criminals (i.e. those arrested but not convicted).*

The analysis suggests that the effectiveness of long term DNA retention is limited.

Because DNA personal data of criminals is to be retained indefinitely, there is a significant risk that the proposed DNA database will cover most of the population and that a universal DNA database will be established by default.

(a) The effectiveness of the retention of DNA personal data of criminals

The table below is from "*Time to reconviction: by gender, 1995-97*"[4]. This includes details of under-21 offenders who are released from prison. The commentary adds "Overall there was little difference in the reconviction rates for those released from prison and those who had served community sentences" so the table shows young male recidivism in general.

The statistics of male young offenders under 21 serving custodial sentences are as follows:

16% of males re-offend within 3 months
35% of males re-offend within 6 months
50% of males re-offend within 9 months
60% of males re-offend within 12 months
67% of males re-offend within 15 months
71% of males re-offend within 18 months
74% of males re-offend within 21 months
77% of males re-offend within 24 months

If the cumulative figures in the table above are extrapolated[5] on a forward yearly basis we find that:

60%	re-offend in	1 year
77%	re-offend in	2 years
82%	re-offend in	3 years
83%	re-offend in	4 years
84%	re-offend in	5 years
84.5%	re-offend in	6 years

So in relation to those with a criminal record, a three to four year retention period for DNA appears optimal in that it would allow most reoffending (83%) to be caught (assuming that the DNA was the only means of identifying the offender). The extra three years retention adds about an additional 2%. **In other words, indefinite retention of DNA personal data on criminals cannot be justified in terms of helping the police in relation to routine crime because if recidivism does not occur within 3-4 years, the retained DNA is unlikely ever to be used again.**

In fact I think the Government's position inferred from these statistics can be simply stated. The police need DNA retention just in case a criminal, in future, commits a serious crime (e.g. murder, rape) beyond the optiman 3-4 year period. Since the police are indefinitely

---

[4] *There are similar cumulative statistics for women and male adult offending; the juvenile stats are at* http://www.statistics.gov.uk/STATBASE/xsdataset.asp?More=Y&vlnk=405&All=Y&B2.x=16&B2.y=7.

[5] *Although different extrapolation techniques will provide different percentages, the actual final percentage – in this case around 84.5% - is not the important point. The important point is the tapering off of to a maximum percentage in about year 3 to 4. Note there is marginal benefit for each year more than a 3-4 year retention period. Extrapolation of the similar statistics for women and male adult offending show the same trend*

retaining DNA personal data for serious crime, it might as well use these data for any future crime.

(b) Will a universal DNA database emerge?

Official statistics also show that "Research recently carried out on men born in 1953 revealed that **one in three** had a conviction before they were 46 years old" A second statistic states that: "Across England and Wales, the rate of men aged 18 or over found guilty of offences in 2005 was **four times higher** than that of women aged 18 and over (55 men per 1,000 population compared with 12 for women)" [6]. So, if one in three males has an offence, and this is four times the women offenders' ratio, we can roughly assume that **one in twelve women** has a conviction.

Ministers have stated in Parliament that "It is not possible to say how many people on the NDNAD (the DNA database) have not been convicted"[7] This is not correct: a simple calculation produces an estimate of about 1.6% of the population[8] (which is increasing as DNA on those who have not been convicted is still being retained).

Assume there is two decades of indefinite retention of criminal records (which is the policy of all main political parties). Thus for every group of 1000 individuals equally divided into 500 men and 500 women, there will 167 male criminals (one third of males) and 42 female criminals (one twelfth of women) and up to 16 "non criminals" (1.6% of 1000) with a DNA sample on the database. This means that between 209 and 225 individuals (or 21%- 22.5% of the sample population) will be on the DNA database.

Note that this estimate ignores the impact of the retention of DNA data relating to those who have died. One of the statutory functions of the DNA database is to identify deceased persons and DNA are retained indefinitely if individual concerned had committed a "recordable offence".

Assume also that in future a technique is developed by any of the law enforcement or national security agencies to map a sample of retained DNA personal data onto the DNA profile of close relatives (e.g. the DNA provider's two parents, and children). Assuming the norm of "2.3 children and 2 parents", a single DNA sample can be expected to cover 4.3 people on average. This means that coverage of 21%-22.5% would in effect map 90%-97% of the population (and this is not taking into account of the indefinite retention of DNA data

---

[6] *Men* http://www.statistics.gov.uk/STATBASE/ssdataset.asp?vlnk=4480&More=Y*: Women* http://www.statistics.gov.uk/cci/nugget.asp?id=1968.

[7] *Hansard, 15 Sep 2008, Column 2070W*

[8] *The ONS state that in 2008, the population in England and Wales was about 54.5 million (http://www.statistics.gov.uk/cci/nugget.asp?ID=6). A statement to Parliament in November 2008, revealed that in March of that year there were "857,366 people on the NDNAD who had been sampled by England and Wales police forces did not have a current criminal record on PNC" (Hansard, 4 Nov 2008 : Column 358W). A simple division tells us that around 1.6% of a random population will have no criminal record but will be on the DNA database. It is difficult to see why the Government could not have provided this statistic when asked.*

of the dead). A more advanced technique that mapped a retained DNA sample to grandparents and grandchildren would imply a multiplier of over 8.

This explains why I think that the DNA database, even though it is mainly limited to indefinite retention of DNA data relating to recordable offence criminals, will eventually span most of the UK population. It is not a question of ***whether***, it is a question of ***when***; this prospect needs only the passage of time and a technical innovation. In other words, the policies of all political parties is for a universal DNA database that could arise, by default.

In the context of DNA, the Science and Technology Parliamentary Select Committee ("Forensic Science on Trial", session 2004-2005) concluded

- "We are concerned that the introduction of familial searching has occurred in the absence of any Parliamentary debate about the merits of the approach and its ethical implications".
- "Any future extension to the applications for which the data in the NDNAD can be used must be subject to public scrutiny".
- "In failing to respond more positively to the calls for independent oversight of the database, the Home Office gave the impression that it was not a high priority."

These recommendations are still current because there is nothing in the Bill that requires Parliamentary scrutiny of familial searching, and nothing in the Bill that limits "extension of applications". This is because the threshold that defines the purposes of the DNA database (e.g. "interest of national security" and "purposes related to the prevention and detection of crime" as in inserted clause 64ZN[9]) is very low with the result that the purposes are very broad in application. **That is why a sunset clause is important; it allows Parliament to re-examine the DNA database in the light of technical advances.**

ENDS

[9] *Page 47, line 20 of the Bill at Second Reading (Commons)*

APPENDIX: ADVERTS

DATA PROTECTION FOR USA AND EUROPEAN PRIVACY OFFICERS

We have developed a course to provide USA and European privacy officers with rounded knowledge of European Data Protection law based on the Directive 95/46/EC and the Privacy & Electronic Communications Directive 2002/58/EC (the latter in the context of e-commerce). An assessment of understanding can be obtained by written exam – this is a variant of the data protection qualification for the UK offered by the ISEB, a qualification body linked to the British Computer Society. The ISEB have told us they are prepared to set an exam if there is demand. If interested please contact ***info@amberhawk.com***.

COURSES FOR DATA PROTECTION OFFICERS IN THE UK

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection. With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, PECR, CCTV, Human Resources, Data sharing) as well as on-site ISEB courses. We are developing a "train your data protection team" offering.

We have a Data Protection Audit courses as well as a course on Level 1 of the Government's Information Assurance Strategy (the HMG Security Framework). If interested please contact us at ***info@amberhawk.com***

COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification. With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies. We are developing a "train your FOI team" offering

If interested please contact us at ***info@amberhawk.com***