Protection of Freedoms Bill

Fact Sheet - Part 1: Regulation of Biometric Data

Chapter 1: Destruction, retention and use of fingerprints and samples etc

The Coalition's Programme for Government states that the Government "*will adopt the protections of the Scottish model for the DNA database"*.

The European Court of Human Rights judgment in the case of *S and Marper* in December 2008 found that the present blanket and indiscriminate indefinite retention of the DNA and fingerprints of innocent people was a breach of Article 8 of the European Convention of Human Rights.

This Chapter contains the revised framework for the retention and destruction of fingerprints and DNA samples and profiles, which aims to restore the overriding presumption that a person is innocent until proven guilty, and to strike the right balance between public protection and safeguarding civil liberties.

Destruction of DNA samples

The Bill makes provision for the destruction of DNA samples, whether from convicted or unconvicted individuals, as soon as a DNA profile is loaded onto the National DNA Database (NDNAD). Furthermore any sample must be destroyed before the end of a 6 month period from when the sample was taken.

The Bill also provides important safeguards to ensure that biometric material is destroyed if it is found that the material was taken unlawfully, following an unlawful arrest or in a case of mistaken identity.

Persons arrests for or charged with a serious offence

As in Scotland, the biometric data of those charged with, but not convicted of, a serious ('qualifying') offence may be retained for an initial period of 3 years, extendable for a single further period of 2 years with the approval of a District Judge (Magistrates' Courts). The new regime will differ from the Scottish model by also allowing for the retention of biometric data following arrest (rather than charge) in certain circumstances and subject to the approval of the new Commissioner for Retention and Use of Biometric Material. Retention following arrest will, in particular, be permitted where the victim of an alleged serious offence is: (a) under 18, (b) a vulnerable adult, or (c) in a close personal relationship with the arrested person.

The Scottish model allows repeated renewals but the Bill allows for only a single extension and therefore avoids any possibility of allowing indefinite retention by the back door.

Persons arrested for or charged with a minor offence
Where a person is arrested for and/or charged with a minor crime, but not convicted of that offence, their DNA profile and fingerprints must be destroyed as soon as the case is discontinued or the person is found not guilty by a court (subject to the completion of a speculative search).

Persons with previous convictions for recordable offence(s)
The provisions in the Bill ensure that any person found to have a previous conviction for a recordable offence (which is an offence punishable by imprisonment or one of around 60 other offences specified in regulations) will have their DNA profile and fingerprints retained indefinitely, regardless of the outcome of the current investigation. There is an exemption for those people with convictions for one minor offence when they were under the age of 18, who are subsequently arrested for another minor offence but not convicted.

Persons under 18 convicted of first minor offence
Modified retention rules apply to children and young people with a single minor conviction or caution. The DNA and fingerprints of juveniles on first conviction, reprimand or warning would be retained for 5 years, if the sentence was non-custodial, or for the length of sentence plus 5 years for those sentenced to immediate youth custody.

Persons given a penalty notice
Where a person accepts a penalty notice, his or her DNA profile and fingerprints may be retained for 2 years, where they have been taken in connection with the investigation of the offence.

National DNA Database Strategy Board
The National DNA Database Strategy Board already exists, but this Chapter put the Board (and the Database itself) on a statutory footing. Membership of the Board includes independent non-police bodies such as the Information Commissioner and the National DNA Database Ethics Group.

The Board will be required to produce guidance to chief officers on the circumstances when DNA samples and profiles should be removed immediately. This guidance will ensure a consistent approach is adopted across England and Wales.

Speculative searches
Where a person's DNA profile and fingerprints would otherwise be due to be destroyed, the Bill allows them to be retained long enough to enable the police to undertake a speculative search against fingerprint and DNA databases to identify matches. Speculative searching ensure suspects can be linked with previous convictions, possibly under different identities, and with crime scenes, including those unrelated to the current investigation.

National security
Although the decision of the European Court of Human Rights judgment in *Marper* did not specifically addresses the issue of retention of biometric material for national security purposes, the Bill makes provisions broadly equivalent to those in PACE – that is, limiting retention periods for national security (including counter-terrorism) purposes to 3 years (6 months in the

case of persons detained under Schedule 7 to the Terrorism Act 2000). Although the police will be permitted to seek further extension where a case for prolonged retention of DNA profiles and fingerprints can be made, this power will be subject to oversight by the new independent Commissioner for Retention and Use of Biometric Material.

Chapter 2: Protection of Biometric Information of Children in Schools Etc.

Chapter 2 of Part 1 contains provisions to protect the biometric data of children when used in schools and colleges. In particular it provides that parents must give their written consent before a school or college can process their child's biometric, and allows children to refuse to provide their data. It also requires that alternative arrangements are made for those children who object or whose parents do not consent to the processing of their biometric data.

Requirement for parental consent

The Coalition's Programme for Government states that the Government "*will outlaw the fingerprinting of children in school without parental permission*".

Schools and colleges use biometric systems, for example automated fingerprint recognition systems, for practical purposes such as running libraries or canteens. The biometric data processed by these systems is regulated by the Data Protection Act 1998 ("DPA"); however there is no explicit requirement in the DPA for parental consent to be gained.

This Chapter provides that schools and colleges must obtain written parental consent before processing biometric data of children under the age of 18 using an automated recognition system – 'parental' in this context also covers those with 'parental responsibility' for the child. These clauses also provide that this consent can be withdrawn in writing at any time.

Child's right to refuse

The DPA requires that schools or colleges must not process a child's biometric data unless one of a number of conditions is met. Although one of the conditions is that the child consents to the processing, this is not the only condition that a school or college could seek to rely on. This leaves open the possibility that a school or college could legally process a child's biometric data without a child's consent.

This Chapter therefore also provides that a school or college must not process a child's biometric data if the child refuses. This applies where the child refuses to physically give their biometric information and also where children verbally or otherwise voice their objection to the processing of their biometric information.

Alternative arrangements

This Chapter further provides that schools and colleges must provide alternative arrangements for children who refuse to allow the processing of their biometric data or whose parents do not give their consent. The alternative arrangements must allow pupils the same level of access to school facilities, etc as a child who accesses such facilities via a biometric system.

Home Office and Department for Education
October 2011