



## Retention of fingerprints and DNA data

Standard Note: SN/HA/4049

Last updated: 14 November 2013

Author: Jacqueline Beard and Sally Lipscombe

Section: Home Affairs

---

A new regime governing the retention of fingerprints and DNA data by the police in England and Wales was introduced by the *Protection of Freedoms Act 2012*. The relevant provisions were brought into force on 31 October 2013. Prior to the commencement of these provisions the police were able to retain fingerprint and DNA data taken from individuals arrested for a recordable offence for an indefinite period, irrespective of whether they were ultimately charged or convicted. Detailed rules are now in place regarding when and for how long the police may retain an individual's DNA data and fingerprints.

This note sets out the current legal framework and outlines the background to the changes made by the *Protection of Freedoms Act 2012*.

Individuals requiring legal advice on the retention of their fingerprints or DNA data should consult an appropriately qualified professional.

This information is provided to Members of Parliament in support of their parliamentary duties and is not intended to address the specific circumstances of any particular individual. It should not be relied upon as being up to date; the law or policies may have changed since it was last updated; and it should not be relied upon as legal or professional advice or as a substitute for it. A suitably qualified professional should be consulted if specific advice or information is required.

This information is provided subject to [our general terms and conditions](#) which are available online or may be provided on request in hard copy. Authors are available to discuss the content of this briefing with Members and their staff, but not with the general public.

**Contents**

- 1 The current law in England and Wales 3**
  - 1.1 Individuals arrested for or charged with “qualifying offences” 3
  - 1.2 Individuals arrested for or charged with minor offences 3
  - 1.3 Adults convicted of an offence 4
  - 1.4 Juveniles convicted of an offence 4
  - 1.5 National security 4
  - 1.6 The Biometrics Commissioner 5
  
- 2 Background to the Protection of Freedoms Act 2012 6**
  - 2.1 The previous legal framework 6
  - 2.2 The human rights challenge in the courts 7
  - 2.3 The Labour Government’s response: the Crime and Security Act 2010 8
  - 2.4 The Coalition’s response: the Protection of Freedoms Act 2012 9
    - The law in Scotland 9
    - The Protection of Freedoms Act 2012 10
  - 2.5 Deletion of data taken and retained before the Act’s provisions came into force 5

## 1 The current law in England and Wales

The general rule under the *Police and Criminal Evidence Act 1984* (PACE) is that the police may not take fingerprints or a non-intimate sample<sup>1</sup> from a person without his consent. However, there are a number of exceptions to this rule, the most important being where a person has been arrested for, charged with or convicted of a recordable offence.<sup>2</sup> In such cases the police can take fingerprints or non-intimate samples without consent.

Under Part 1 of the *Protection of Freedoms Act 2012* (the “2012 Act”), there is a presumption that fingerprints and DNA data taken by the police under PACE or with the individual’s consent must be destroyed unless one or more of the exceptions set out in the 2012 Act applies, in which case the police can retain the material for a specified period. Some of the key circumstances in which data may be retained are set out below.

### 1.1 Individuals arrested for or charged with “qualifying offences”

Section 3 of the 2012 Act inserts new section 63F into PACE. It deals with those arrested for or charged with – but not convicted of – certain serious sexual, violent or terrorist offences known as “qualifying offences”.<sup>3</sup> If the individual who has been arrested or charged has a previous conviction for a recordable offence, then the police can retain his data indefinitely. If the individual has no previous convictions, then the retention arrangements will depend on whether he was charged or only arrested:

- if the individual was **charged** with a qualifying offence, then the police can retain his data for three years;
- if he was only **arrested** for a qualifying offence (but not charged), then the police can retain his material for three years but only if they have first obtained the consent of the new Independent Commissioner for the Retention and Use of Biometric Material (appointed under section 20 of the 2012 Act).<sup>4</sup>

The police can apply to the magistrates’ courts for a single two year extension in respect of data subject to an initial three year retention period. The police have a right of appeal to the Crown Court against a decision not to grant an extension, and the person to whom the material belonged has a similar right of appeal against a decision to permit an extension.

### 1.2 Individuals arrested for or charged with minor offences

Section 4 of the 2012 Act inserts new section 63H into PACE which deals with those who are arrested for or charged with – but not convicted of - a minor offence (i.e. a recordable offence that is not a qualifying offence). Data taken from such people must be destroyed, unless

---

<sup>1</sup> Namely a sample of hair other than pubic hair, a sample taken from a nail or from under a nail, a swab taken from any part of a person’s body (excluding their genitals or a body orifice other than the mouth), a saliva sample or a skin impression (PACE, s65(1))

<sup>2</sup> A recordable offence is any offence punishable with imprisonment and any other offence specified in the Schedule to the National Police Records (Recordable Offences) Regulations 2000, SI 2000/1139 (as amended)

<sup>3</sup> The full list of qualifying offences is set out in section 65A of PACE, as inserted by [section 7 of the Crime and Security Act 2010](#) (section 7 was brought into force by the Coalition Government on 7 March 2011 and is one of the only DNA provisions in the 2010 Act to have been given legal force)

<sup>4</sup> The police may apply to the Commissioner to retain such data if the victim of the alleged offence was (at the time of the offence) under the age of 18, a vulnerable adult or in a close personal relationship with the arrested person. The police may also apply where they consider that retention is necessary for the prevention or detection of crime. Notice of any application to the Commissioner must also be given to the person from whom the data was taken, and that person may make representations to the Commissioner in respect of the application. If the Commissioner does not give his consent then the data cannot be retained.

they have previously been convicted of a recordable offence (other than an “excluded offence”<sup>5</sup>) in which case the material can be retained indefinitely.

### **1.3 Adults convicted of an offence**

Under section 5 (which inserts new section 63I into PACE), data from an adult convicted of a recordable offence (whether it is a qualifying offence or a minor offence) can be retained indefinitely. “Convicted” for these purposes includes being cautioned, being found not guilty by reason of insanity, or being found to be under a disability (i.e. unfit to plead) and to have done the act charged.

### **1.4 Juveniles convicted of an offence**

Under section 5, data from those convicted of a qualifying offence committed when aged under 18 can be retained indefinitely. Similar provision is made for the indefinite retention of data taken from those convicted of a minor offence (other than a first minor offence) committed when aged under 18. Again, “convicted” includes being reprimanded or warned, being found not guilty by reason of insanity, or being found to be under a disability and to have done the act charged.

Under section 7 (which inserts new section 63K into PACE), data from those convicted of a first minor offence committed when aged under 18 can be retained for the following periods:

- where the individual is given a custodial sentence of less than five years in respect of the offence, the data can be retained until the end of the period consisting of the term of the sentence plus five years;
- where he is given a custodial sentence of five years or more, the data may be retained indefinitely;
- where he is given a sentence other than a custodial sentence, the data may be retained for five years.

If the offender commits a further recordable offence during any of these retention periods then his data may be retained indefinitely.

### **1.5 National security**

Section 9 (which inserts new section 63K into PACE) makes provision for the retention of material for the purposes of national security. Where a person’s data would otherwise have to be destroyed, the police may retain it for up to two years where the responsible chief officer of police determines that it is necessary to do so for the purposes of national security. This is referred to as a “national security determination”. National security determinations can be renewed for up to two years at a time; there is no limit on the number of times that a national security determination can be renewed.

The new Independent Commissioner for the Retention and Use of Biometric Material (appointed under section 20 of the 2012 Act) is responsible for keeping every national security determination made by the police under review. The police must send him a copy of every determination they make or renew, together with the reasons for making or renewing it, within 28 days of making or renewing it. They must also provide the Commissioner with such

---

<sup>5</sup> An “excluded offence” is defined as a recordable offence which is not a qualifying offence, is the only recordable offence of which the person has been convicted, was committed when the person was aged under 18 and did not result in a custodial sentence of five years or more

documents and information as he may require for the purpose of reviewing national security determinations.

If, on reviewing a national security determination, the Commissioner concludes that it is not necessary to retain the data that the determination relates to, then he may order the destruction of the material (provided that it is not otherwise capable of being lawfully retained).

Section 22 of the 2012 Act requires the Secretary of State to issue statutory guidance on the making and renewal of national security determinations. The guidance was issued by the Home Office in June 2013: [Protection of Freedoms Act 2012: Guidance on the making or renewing of national security determinations allowing the retention of biometric data](#).

## **1.6 The Biometrics Commissioner**

Information about the Independent Commissioner for the Retention and Use of Biometric Material (the “Biometrics Commissioner”) can be found on the gov.uk website page: [Biometrics Commissioner](#).

The guidance document, [Applications for biometric retention: what you should know](#), 11 November 2013, provides an explanation of how and when applications can be made to the commissioner to keep the DNA profile and fingerprint records of a person who has been arrested for, but not charged with a qualifying offence, what the process means for those individuals who are the subject of such an application and how they can make representations to the commissioner.

The policy paper, [Principles for assessing applications for biometric retention](#), 11 November 2013, sets out the principles which will inform the Commissioner’s approach to such applications and the factors to which he will attach significance when determining them.

## **1.7 Deletion of data taken and retained before the Act’s provisions came into force**

Before the relevant sections of the 2012 Act were brought into force, DNA and fingerprints that had previously been taken and were being stored, which would not meet the requirements of the Act, were deleted from the relevant databases. Secondary legislation was issued by the Secretary of State under section 25 of the 2012 Act which set out the framework for the destruction of such data.<sup>6</sup>

Lord Taylor of Holbeach said in a Written Ministerial Statement on 24 October 2013:

The Government has now delivered its commitment to reform the retention of DNA and fingerprint records by removing innocent people from the databases, and adding the guilty.

1,766,000 DNA profiles taken from innocent adults and children have been deleted from the National DNA Database. 1,672,000 fingerprint records taken from innocent adults and children have been deleted from the national fingerprint database. 7,753,000 DNA samples containing sensitive personal biological material, no longer

---

<sup>6</sup> [The Protection of Freedoms Act 2012 \(Destruction Retention and Use of Biometric Data\) \(Transitional Transitory and Saving Provisions\) Order 2013](#), SI 2013/1813 and [The Protection of Freedoms Act 2012 \(Destruction Retention and Use of Biometric Data\) \(Transitional Transitory and Saving Provisions\) \(Amendment\) Order 2013](#), SI 2013/2580

needed as a DNA profile has been obtained, have been destroyed. 480,000 of the DNA profiles removed as part of this programme were taken from children.

At the same time, 6,800 convicted murderers and sex offenders, not on the database under the previous Government, have had their DNA taken and added to the database. These records will be kept permanently, as will those of every convicted adult on the database, to ensure our databases remain a powerful tool for fighting crime.

Now that our DNA and fingerprint databases meet the requirements set out in Part 1, Chapter 1 of the Protection of Freedoms Act 2012, these provisions will be commenced, on 31 October.

The National DNA Database (NDNAD) annual report for 2012-13 was today published on the Home Office website, providing information for the public on the routine operation and effectiveness of the database, and on the programme to delete innocent people in preparation for the Protection of Freedoms Act. This report is an important part of the Government's aim for transparency and public confidence in the use of DNA.

The figures in the first part of the report show the size of the NDNAD to 31 March 2013, part way through work to delete DNA profiles in line with the Protection of Freedoms Act. Following the deletions described above, the NDNAD will now be considerably smaller. Part two of the report provides more detailed information on these deletions.<sup>7</sup>

Further information on the work to delete data can be found in the [National DNA Database Strategy Board Annual Report 2012-13](#) and in the Home Office's [Policy paper: Protection of Freedoms Act 2012: how DNA and fingerprint evidence is protected in law](#), 4 April 2013.

## **2 Background to the Protection of Freedoms Act 2012**

### **2.1 The previous legal framework**

The previous legal framework on taking and retaining fingerprints and DNA data was set out in section 64 of the *Police and Criminal Evidence Act 1984* (PACE), now repealed by the *Protection of Freedoms Act 2012*.

This legislation did not specify any time limits for retention or any procedure by which data could be removed from police records. The police were therefore able to retain fingerprint and DNA data taken from individuals arrested for a recordable offence for an indefinite time period.

Time limits and a removal procedure (known as the "exceptional case procedure") were set out in non-statutory guidance issued by the Association of Chief Police Officers (ACPO). In accordance with this guidance, police practice was to delete DNA data once the individual it relates to attained (or was deemed to have attained) 100 years of age.<sup>8</sup> The police would usually only agree to delete data prior to this date by way of the exceptional case procedure:

Chief Officers have the discretion to authorise the deletion of any specific data entry on the PNC 'owned' by them. They are also responsible for the authorisation 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.

---

<sup>7</sup> [HL Deb 24 October 2013 cWS109](#)

<sup>8</sup> ACPO, [Retention Guidelines for Nominal Records on the Police National Computer](#), March 2006, para 3.1

(...)

Exceptional cases will by definition be rare. They might include cases where the original arrest or sampling was found to be unlawful. Additionally, where it is established beyond doubt that no offence existed, that might, having regard to all the circumstances, be viewed as an exceptional circumstance.<sup>9</sup>

## 2.2 The human rights challenge in the courts

Article 8 of the *European Convention on Human Rights* provides:

### Right to respect for private and family life

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.

In *R v Chief Constable of South Yorkshire ex p S and Marper*,<sup>10</sup> the domestic courts considered whether the indefinite retention of fingerprints and DNA data under PACE was compatible with the *European Convention on Human Rights*. Fingerprints and DNA samples had been taken from S, an 11 year old boy who was acquitted of robbery, and from Michael Marper, a man against whom proceedings for harassment of his partner had been discontinued. In both cases, the police proposed to retain the samples, while S and Marper argued that they should be destroyed. Having been unsuccessful in both the Divisional Court and the Court of Appeal, the claimants' further appeal to the House of Lords was also dismissed. The House of Lords held that any interference with rights under Article 8(1) by retention of fingerprints and DNA samples was modest, and was objectively justified under Article 8(2) as being necessary for the prevention of crime and the protection of the rights of others.

S and Marper then lodged an application with the European Court of Human Rights. The Grand Chamber's judgment was handed down on 4 December 2008.<sup>11</sup> The Court accepted that the retention of fingerprint and DNA information pursued a legitimate purpose, namely the detection and prevention of crime, but held unanimously that the retention and storage of the applicants' fingerprints and DNA samples was disproportionate and not "necessary" in a democratic society. Article 8 had therefore been violated. In considering whether the indefinite retention of samples from all suspected but unconvicted persons was proportionate and struck a fair balance between competing private and public interests, the Court held:

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;

---

<sup>9</sup> Ibid, Appendix 2

<sup>10</sup> Divisional court ruling at [2002] EWHC 478 (Admin), Court of Appeal ruling at [2002] EWCA Civ 1275, and House of Lords ruling at [2004] UKHL 39

<sup>11</sup> *Case of S. And Marper v The United Kingdom*, Applications nos. 30562/04 and 30566/04

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 ...; 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.

(...)

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.

Jack Straw, the then Justice Secretary, made the following comment on the judgment:

It [suggests] that distinctions should be made between the nature of offences for which samples have been taken, and discusses whether they should be time-limited and whether there should be an independent review. Those matters will be considered by my right hon. Friend the Home Secretary in consultation across Government. We have an obligation to report initially to the Council of Ministers and the Council of Europe by March.<sup>12</sup>

### 2.3 The Labour Government's response: the Crime and Security Act 2010

The Labour Government's legislative response to the judgment was set out in the *Crime and Security Act 2010*. Note, however, that the relevant section of the 2010 Act was never brought into force.

A white paper on DNA retention was published on 7 May 2009.<sup>13</sup> It invited views on the content of proposed regulations that would set out a new framework for the retention of fingerprints and DNA in England and Wales. Its key proposals included destroying all DNA samples<sup>14</sup> taken on arrest, and replacing the blanket retention of DNA profiles<sup>15</sup> with a differentiated approach based on factors such as age, offence type and conviction.

On 11 November 2009, the then Home Secretary Alan Johnson made a written ministerial statement outlining a revised set of proposals for the retention of fingerprint and DNA data.<sup>16</sup> The revised proposals were subsequently introduced as clauses 2 to 20 of the *Crime and*

---

<sup>12</sup> [HC Deb 4 Dec 2008 c226](#)

<sup>13</sup> Home Office, *Keeping the right people on the DNA database*, May 2009

<sup>14</sup> "DNA samples" are the physical samples taken from an individual, such as a mouth swab, hair or blood. DNA samples are currently retained indefinitely and stored in secure sterile laboratories.

<sup>15</sup> "DNA profiles" are the computerised records of the pattern of DNA characteristics taken from DNA samples. DNA profiles are currently retained indefinitely on the NDNAD and appear as numeric codes on the Police National Computer.

<sup>16</sup> [HC Deb 11 November 2009 cc25-28WS](#). Accompanying the statement was a new "review of the evidence in relation to a policy of DNA record retention": see Home Office, *DNA Retention Policy: Re-Arrest Hazard Rate Analysis*, November 2009

*Security Bill*, which had its first reading on 19 November 2009. Detailed background is set out in Library Research Papers [09/97 Crime and Security Bill](#) (section 2) and [10/22 Crime and Security Bill: Committee Stage Report](#) (section 3.1), and in Lords Library Note [2010/010 Crime and Security Bill](#) (section 2).

The Bill received Royal Assent on 8 April 2010 to become the [Crime and Security Act 2010](#). Section 14 would have amended section 64 of the *Police and Criminal Evidence Act 1984* to introduce a more limited framework for the retention of fingerprints and DNA data. For example, the police would have been able to retain data from adults arrested but not convicted of an offence for six years. Data from under those aged under 18 convicted of a single minor offence would have been retained for five years.<sup>17</sup>

However, section 14 of the 2010 Act was never brought into force due to the change in Government shortly after the Act received Royal Assent.

## **2.4 The Coalition's response: the Protection of Freedoms Act 2012**

Following the 2010 election, the Coalition Government indicated that it would be legislating to "adopt the protections of the Scottish model for the DNA database".<sup>18</sup>

### ***The law in Scotland***

In very brief terms, the Scottish framework for the retention of fingerprints and DNA is as follows:

- fingerprint and DNA data from convicted individuals is retained indefinitely;
- data from individuals prosecuted for certain sexual or violent offences may be retained for three years (whether or not they are convicted), with chief police constables able to apply to the sheriff court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of any particular person's data); and
- data from individuals arrested for any other offences must be destroyed immediately if they are not convicted or if they are granted an absolute discharge.

More detailed guidance on the Scottish system is available in a briefing note prepared by the Scottish Parliament Information Centre.<sup>19</sup>

The European Court of Human Rights drew specific attention to the Scottish system in its judgment in *S and Marper*:

109. The current position of Scotland, as a part of the United Kingdom itself, is of particular significance in this regard. As noted above ... , 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

---

<sup>17</sup> See paragraph 51 of the [Explanatory Notes to the Crime and Security Act 2010](#) for a detailed overview of section 14

<sup>18</sup> Cabinet Office, [The Coalition: our programme for government](#), May 2010, p11

<sup>19</sup> Scottish Parliament Information Centre Briefing 09/30, [Criminal Justice and Licensing \(Scotland\) Bill: Fingerprint and DNA Data](#), 1 May 2009

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.<sup>20</sup>

### ***The Protection of Freedoms Act 2012***

The Government's proposals were introduced in Part 1 of the *Protection of Freedoms Bill*, which had its first reading on 11 February 2011. Detailed background is set out in Library Research Papers [11/20 Protection of Freedoms Bill](#) (section 2) and [11/54 Protection of Freedoms Bill: Committee Stage Report](#) (section 4.1), and in Lords Library Note [2011/033 Protection of Freedoms Bill](#) (section 3.1).

The Bill received Royal Assent on 1 May 2012 to become the *Protection of Freedoms Act 2012*. Most of the provisions in Part 1 of the Act, which relate to the destruction and retention of DNA data, came into force on the 31 October 2013.<sup>21</sup>

The Act repealed both section 64 of PACE and section 14 of the *Crime and Security Act 2010*. It inserted a number of new sections into PACE to replace the previous indefinite retention regime with a more restricted one. Please see paragraphs 83 to 139 of the [Explanatory Notes to the 2012 Act](#) for a full overview.

---

<sup>20</sup> [Case of S. And Marper v The United Kingdom](#), Applications nos. 30562/04 and 30566/04, paragraphs 36 and 109-110

<sup>21</sup> [The Protection of Freedoms Act 2012 \(Commencement No 7\) Order 2013](#), SI 2013/1814