The Scottish Government introduced the Criminal Justice and Licensing (Scotland) Bill in the Parliament on 5 March 2009. It includes provision to extend existing police powers in relation to the retention of certain types of forensic information – including fingerprint and DNA data.

This briefing considers, in light of the proposals in the Bill, police powers and practices in relation to the acquisition and use of fingerprint and DNA data.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>POLICE USE OF FORENSIC INFORMATION</td>
<td>4</td>
</tr>
<tr>
<td>FINGERPRINT DATA</td>
<td>4</td>
</tr>
<tr>
<td>DNA DATA</td>
<td>5</td>
</tr>
<tr>
<td>CURRENT POLICE POWERS</td>
<td>6</td>
</tr>
<tr>
<td>Scotland</td>
<td>6</td>
</tr>
<tr>
<td>England and Wales</td>
<td>8</td>
</tr>
<tr>
<td>PROPOSALS TO CHANGE POLICE POWERS IN SCOTLAND</td>
<td>10</td>
</tr>
<tr>
<td>Review and Consultation</td>
<td>10</td>
</tr>
<tr>
<td>The Bill</td>
<td>11</td>
</tr>
<tr>
<td>Retention of Data and Alternatives to Prosecution</td>
<td>12</td>
</tr>
<tr>
<td>SOURCES</td>
<td>14</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

- Scotland – current police powers in relation to fingerprint and DNA data:
  - the police have various powers to take fingerprints and DNA samples from suspects. Such forensic information can be analysed, checked against existing records on relevant databases, and added to such databases for future reference
  - where there is a criminal conviction, any fingerprint or DNA data which have been obtained from an offender can be retained indefinitely. However, all fingerprint data taken from a suspect must be deleted from databases and destroyed if the suspect is not subsequently convicted in a criminal court. This was, until quite recently, also the position in relation to DNA data taken from a suspect who is not subsequently convicted
  - the rules on the retention of DNA data (but not fingerprint data) were modified by the Police, Public Order and Criminal Justice (Scotland) Act 2006. Since the changes came into force, in January 2007, DNA data obtained from a suspect who is prosecuted in the criminal courts for any of a wide range of sexual or violent offences may be retained for a period after the conclusion of criminal proceedings, even if the suspect is not convicted
  - where there is no conviction but the extended retention powers do apply, DNA data must still be deleted from databases and destroyed at some point. This must be done: (a) within three years of the date on which the criminal proceedings were concluded; or (b) by any later date set by a sheriff following an application by a chief constable to extend the retention period

- England and Wales – current police powers in relation to fingerprint and DNA data:
  - a major difference from the position in Scotland is that fingerprint and DNA data obtained from a suspect can, irrespective of whether the suspect is prosecuted or convicted, be retained indefinitely
  - in December 2008 the European Court of Human Rights held that the legislative regime governing the retention of fingerprint and DNA data taken from suspects in England and Wales is in breach of Article 8 of the European Convention on Human Rights (right to respect for private and family life) – the case related to individuals who had not been convicted of an offence
  - in holding that the rules in England and Wales violate the convention, the European Court of Human Rights said that it was “struck by the blanket and indiscriminate nature of the power of retention”. It also highlighted, with some indication of approval, the more restricted retention powers in Scotland
  - since the European Court of Human Rights’ ruling, the UK Government has indicated that it will implement some changes immediately and consult on other proposals to amend the current rules on retention in England and Wales

- Scotland – changes set out in the Criminal Justice and Licensing (Scotland) Bill seek to:
  - apply the current extended DNA retention powers, introduced by the Police, Public Order and Criminal Justice (Scotland) Act 2006, to fingerprint data (and various other types of print such as palm prints)
  - establish extended powers of retention, covering both fingerprint and DNA data, obtained from children who are dealt with by way of the children’s hearings system after committing sexual or violent offences
  - clarify the purposes for which fingerprint and DNA data obtained by the police can be used
POLICE USE OF FORENSIC INFORMATION

The use of forensic information during the investigation and prosecution of crime is not restricted to data on the personal characteristics of individuals (e.g. it may also involve the analysis of paint, glass or fibre samples recovered from a crime scene or accused person). However, the use of forensic information containing details of personal characteristics (including fingerprints and DNA data) raises particular issues relating to individual privacy.

A 2007 report by the Nuffield Council on Bioethics noted that:

"Fingerprints, footprints and fragments of fibre have been used in the investigation and prosecution of crime since at least the end of the 19th Century. However, it is the development over the past two decades of the science and technology underpinning genetic ‘fingerprinting’ and now DNA profiling that has been the main reason for the dramatic increase in the use of bioinformation in the investigation and prosecution of crime.” (para 1.1)

Forensic information containing details of personal characteristics (or ‘bioinformation’) includes DNA data, voice analysis data, fingerprints and other body prints (e.g. palm prints). This briefing focuses on fingerprint and DNA data.

Police use of fingerprint and DNA data includes the comparison of samples recovered from a crime scene or victim, with samples taken directly from a suspect or data stored on a database. Such comparisons can, for example, help establish the presence of a suspect at a crime scene.

The Police, Public Order and Criminal Justice (Scotland) Act 2006 established a new Scottish Police Services Authority (SPSA) providing various common services to all Scottish police forces. Since April 2007, the SPSA has included forensic services, providing a range of services including crime scene examination, DNA analysis and fingerprint analysis. Further information about SPSA Forensic Services is available on its website.

FINGERPRINT DATA

Despite advances in the analysis and use of DNA, fingerprint data is still the main type of bioinformation used within the criminal justice system. Impressions of a suspect’s ten fingerprints (known as ‘tenprints’) can, for example, be compared with impressions left at a crime scene.

The gradual introduction of Livescan terminals (since 1997) has allowed the police in Scotland to obtain fingerprint impressions from people electronically – by the person placing a hand on a glass plate. The information captured in this way is sent to a database. An automated fingerprint recognition system can be used to highlight potential matches between tenprints and crime scene marks. Potential matches are then examined by fingerprint officers to verify any potential identification.

Since December 2006, the police in Scotland, England and Wales have shared a computerised system (known as IDENT1) which hosts various bioinformation databases. These include a

---

2 Although fingerprint identifications are normally accepted as accurate, disputes can arise where, for example, there is only a partial crime scene sample which provides limited information for comparison with tenprints (different countries have different standards for confirming a match). Further information about the difficulties associated with interpreting fingerprint information is provided in the 2007 report by the Nuffield Council on Bioethics (paras 2.2 to 2.4).
joint fingerprint database which can be accessed by police in Scotland and other parts of the UK. It has been reported that the UK’s ‘National Tenprint Collection’ (hosted on IDENT1) holds more than 6.5 million sets of fingerprints, incorporating 20% of the UK male population and 5% of the female population (Nuffield Council on Bioethics 2007, para 1.17).

DNA DATA

The above mentioned report by the Nuffield Council on Bioethics (2007) stated that:

“In general, the taking and retention of DNA is seen as far more ‘sensitive’. This is because fingerprints cannot reveal information beyond identity, whereas with DNA there is the possibility of deriving additional information about an individual by further analysis of their DNA, and about family relationships by comparing profiles.” (para 1.19)

The term ‘DNA data’ is used in this briefing to cover both DNA samples and DNA profiles. A DNA sample is a biological sample from which a DNA profile may be obtained. A DNA profile is a record of some of the information contained within a DNA sample. The Nuffield Council on Bioethics (2007) has pointed out that this difference can be important when considering ethical issues relating to the use and retention of DNA data:

“It is of crucial importance to understand the distinction between a biological sample and a DNA profile. The former is the actual biological sample of body cells taken from a crime scene or from a suspect or a volunteer during an investigation. The latter is a string of numbers stored on the NDNAD (…). Generally, use and retention of a DNA profile raises far fewer ethical concerns than the use and retention of the biological sample. The DNA profile characterises only certain very restricted parts of a person’s total DNA, and these areas of DNA have been selected largely because they provide no information beyond identifying the individual. Thus access to an individual’s profile will not reveal anything of interest about that individual, beyond identification and gender (…) though with the rapid advancement of genetic analysis, and the decreasing cost of profiling greater sequences of DNA, it may not always remain so. The biological sample itself contains the whole genetic sequence of an individual, and is therefore far more sensitive in respect of privacy. Potentially, it might reveal personal, familial and health information, and perhaps even information about behavioural traits.” (para 1.12)

The UK’s National DNA Database (NDNAD), based in Birmingham, contains information on more than 5% of the UK population. It is, in terms of percentage coverage of the population, the largest forensic DNA database in the world. A separate Scottish DNA Database is based in Dundee. DNA profiles obtained from samples taken by the police in Scotland are sent to the NDNAD, as well as being stored on the Scottish DNA Database.

---

3 The NDNAD is the UK’s National DNA Database (see below). DNA profiles may also be stored on other relevant databases (eg the Scottish DNA Database).
4 It was, until quite recently, also the largest in terms of the number of DNA profiles held. However, it has been reported that in the last few years the FBI’s CODIS database in the USA, although containing information on a much smaller proportion of the country’s population, overtook the NDNAD in relation to number of profiles held (Nuffield Council on Bioethics 2007, para 1.22).
5 Northern Ireland also has its own DNA Database.
CURRENT POLICE POWERS

Scotland

The police in Scotland have the power to take fingerprints and DNA samples from suspects who have been arrested and are in custody; or who are detained on suspicion of committing an offence punishable by imprisonment. The police also have powers allowing them to obtain such forensic information from individuals who have been convicted of an offence (eg where fingerprints or DNA samples were not taken prior to conviction).

The above forensic information can be analysed, checked against existing records on relevant databases, and added to such databases for future reference.

In 2005, a response from those running the Scottish Police DNA Database to an earlier Scottish Executive consultation described police practice in relation to taking DNA samples:

“Although the legislation allows police officers to obtain samples from those arrested or detained for any offence, police officers in Scotland currently obtain mouth swabs routinely from suspects arrested or detained for sexual offences, violence and theft. Police officers are also instructed to obtain mouth swabs at their discretion during the investigation of minor offences: for instance, where police officers believe that such sampling will potentially yield further intelligence.” (p 1)

Where there is a criminal conviction, any fingerprint and DNA data which have been obtained from the offender can be retained indefinitely. However, until quite recently, all fingerprint and DNA data taken from a suspect (including both DNA samples and DNA profiles) were deleted from databases and destroyed if the suspect was not subsequently convicted in a criminal court. Thus, forensic information obtained from a suspect was destroyed if, for example: (a) no proceedings were taken; (b) the suspect was dealt with by way of some alternative to prosecution (eg a fiscal fine); (c) a prosecution ended in a verdict of not guilty or not proven; or (d) the suspect was dealt with by way of the children’s hearings system.

The possibility of allowing the retention of forensic information, obtained from suspects, in a wider range of circumstances was considered during the parliamentary passage of the Police, Public Order and Criminal Justice (Scotland) Act 2006. A section added during stage 3 consideration by the Scottish Parliament extended police retention powers in relation to DNA but not fingerprint data. A briefing prepared in advance of stage 3 set out the background to that debate – Police Retention of Prints and Samples – Updated (McCallum 2006).

The extended retention powers introduced by the Police, Public Order and Criminal Justice (Scotland) Act 2006 apply only where a suspect is prosecuted in the criminal courts for a ‘relevant sexual offence’ or a ‘relevant violent offence’. In such circumstances, DNA data obtained from the suspect may be retained for a period of time after the conclusion of criminal proceedings, even though the suspect was not convicted. Thus, for example, the extended retention powers apply to people (including children) who are prosecuted for relevant offences.

---

6 See section 18 of the Criminal Procedure (Scotland) Act 1995.
7 See sections 19 and 19A of the Criminal Procedure (Scotland) Act 1995.
8 In practice, forensic records relating to old or minor convictions are periodically weeded and destroyed.
9 The relevant provisions of the Police, Public Order and Criminal Justice (Scotland) Act 2006 inserted a new section 18A into the Criminal Procedure (Scotland) Act 1995. The extended powers in relation to DNA data have been in force since January 2007.
but found not guilty in the criminal courts, but do not apply to children dealt with through the children’s hearings system for such offences (irrespective of the outcome of any hearing).

Where there is no conviction but the extended retention powers do apply, DNA data must still be deleted from databases and destroyed at some point. This must be done: (a) within three years of the date on which the criminal proceedings were concluded; or (b) by any later date set by a sheriff following an application by a chief constable to extend the retention period. A sheriff may, if satisfied that there are reasonable grounds for doing so, make an order delaying the destruction date by up to two years. This destruction date can be further delayed by a sheriff where a chief constable makes a further application to extend the retention period.

As noted, the extended retention powers for DNA data apply only where a suspect is prosecuted for a relevant sexual offence or a relevant violent offence.

- ‘relevant sexual offence’ – includes a wide range of common law and statutory sexual offences (eg rape, indecent assault and child pornography offences) but not all offences which may involve a sexual element (eg if a case involving sexual exposure is prosecuted as a breach of the peace)
- ‘relevant violent offence’ – includes a wide range of violent offences (eg murder, assault and fire raising) but not all offences which may involve some element of violence (eg breach of the peace) or may be intended to prevent violence (eg offences prohibiting the carrying of knives and offensive weapons in public)

It should be noted that the Sexual Offences (Scotland) Bill (as introduced in the Scottish Parliament on 17 June 2008) includes provisions which would amend the definition of a relevant sexual offence. At present, sexual offending is prosecuted under a wide range of common law and statutory offences. The Sexual Offences (Scotland) Bill seeks to provide a statutory framework for sexual offences, so that most offending of a sexual nature will in future be prosecuted under one of the offences in that bill. In light of this, it seeks to amend the definition of relevant sexual offence to include the new sexual offences which it makes provision for.

The police may also, during the investigation of a crime, obtain fingerprints and DNA data from people who are not identified as suspects but who agree to provide such forensic information on a voluntary basis (eg where the police ask people in a particular neighbourhood to provide DNA samples as a way of eliminating potential suspects). Such information can be retained by the police only with the consent of the person providing it. This consent can be withdrawn at any time.

Police officers across the UK are able to access databases containing fingerprint and DNA data obtained by police officers in different parts of the UK (eg English police forces accessing information obtained by Scottish police forces and vice versa). However, the rules of the part of the UK where the police obtained the information still determine if and when it must be deleted from a database. For example, although the UK and Scottish DNA databases are linked, with police across the UK having access to information stored on both databases, different rules apply to the retention of DNA data collected by police in Scotland and the police in England and Wales. Even where DNA data is included on the NDNAD, the Scottish rules apply to the retention of DNA profiles on that database if they were obtained by the police in Scotland. This can result in Scottish sourced DNA profiles being deleted from the NDNAD in circumstances

---

10 The extended retention provisions use the definitions of ‘relevant sexual offence’ and ‘relevant violent offence’ set out in section 19A(6) of the Criminal Procedure (Scotland) Act 1995.

11 The retention rules applying in England and Wales are outlined below.
where those profiles would not be deleted if they had been collected by the police in England and Wales.

**England and Wales**

In relation to fingerprint and DNA data obtained by the police from a suspect in a criminal investigation, the relevant provisions of the Police and Criminal Evidence Act 1984 originally required the destruction of such data if the suspect was subsequently cleared of the offence, or if there was a decision not to prosecute. However, a series of amendments to the provisions of the 1984 Act significantly changed the law in this area. As a result, the current position is that where the police in England and Wales have lawfully obtained fingerprint or DNA data from a suspect, they are entitled to retain that information indefinitely, irrespective of whether the suspect is prosecuted or convicted. The relevant statutory provisions provide that data retained under these powers can be used only 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”.

In December 2008 the European Court of Human Rights held, in the case of *S and Marper v The United Kingdom*, that the legislative regime governing the retention of fingerprint and DNA data taken from suspects in England and Wales is in breach of Article 8 of the European Convention on Human Rights (right to respect for private and family life). Article 8 provides that:

“(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.”

The European Court of Human Rights stated that:

“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 (…). 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 (…). The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse (…). The above considerations are especially valid as regards the protection of special categories of more sensitive data (…) 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 (…).”

---

12 See section 64 of the Police and Criminal Evidence Act 1984 (as amended by various pieces of legislation including the Criminal Justice and Police Act 2001 and the Criminal Justice Act 2003).
13 The police have more restricted powers to retain fingerprint or DNA data obtained from a person who is not suspected of committing an offence (see sections 64(3) to 64(3AD) of the Police and Criminal Evidence Act 1984).
14 Section 64(1A) of the Police and Criminal Evidence Act 1984.
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 (…). 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.” (European Court of Human Rights 2008, paras 103-104)

In holding that the current rules in England and Wales: (a) do constitute an interference with the rights protected under Article 8(1); and (b) that such interference is not justified under Article 8(2), the European Court of Human Rights said that it was:

“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 (…); 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.” (European Court of Human Rights 2008, para 119)

In criticising the position in England and Wales, the European Court of Human Rights also highlighted the different legal regime applying in Scotland:

“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.

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 (…). 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.” (European Court of Human Rights 2008, paras 109-110)

Since the European Court of Human Rights’ ruling, the UK Government has indicated that it will implement some changes immediately and consult on other proposals to amend the current rules on retention in England and Wales. During a speech in December 2008, the Home Secretary said that:

“There is more we can do to strengthen the dividing line between guilt and innocence. For those who have committed a serious offence, our retention policies need to be as tough as possible. But for others, including children, I am convinced
that we need to be more flexible in our approach. The DNA of children under 10 – the age of criminal responsibility – should no longer be held on the database. There are around 70 such cases, and we will take immediate steps to take them off. For those under the age of 18, I think we need to strike the right balance between protecting the public and being fair to the individual. There’s a big difference between a 12 year old having their DNA taken for a minor misdemeanour and a 17 year old convicted of a violent offence, and next year I will set out in a White Paper on Forensics how we ensure that that difference is captured in the arrangements for DNA retention. We will consult on bringing greater flexibility and fairness into the system by stepping down some individuals over time – a differentiated approach, possibly based on age, or on risk, or on the nature of the offences involved. That may mean letting the 12 year old I mentioned come off the database once they reach adulthood. And it could mean limiting how long the profiles of those who have been arrested but not convicted of an offence could be retained.” (UK Government 2008)

Further information on the position in England and Wales (including the ruling by the European Court of Human Rights) is set out in a paper produced by the House of Commons Library – Retention of Fingerprints and DNA Samples (Almandras 2008).

PROPOSALS TO CHANGE POLICE POWERS IN SCOTLAND

Review and Consultation

In 2007, the Scottish Government asked a forensics expert (Professor James Fraser) to review the operation and effectiveness of the legislative regime governing police powers in relation to the acquisition, use and destruction of fingerprint and DNA data (‘the Fraser Review’). He was directed to consider such powers in so far as they relate to:

- individuals who are prosecuted in the criminal courts for sexual or violent offences but are not convicted
- individuals who, in being dealt with by a children’s hearing, accept that they have committed sexual or violent offences, or are found by a sheriff to have committed such offences

He was asked, following such consideration, to identify options for reforming Scots law, by making appropriate provision for a delay in the destruction of such forensic information, in order to enhance crime prevention and detection capability. Responses to the Fraser Review are available online (Scottish Government 2008a).

In September 2008 the Scottish Government published the review report – Acquisition and Retention of DNA and Fingerprint Data in Scotland (Fraser 2008) (‘the Fraser Report’). It set out eight recommendations covering the following areas:  

- governance arrangements for fingerprint and DNA databases in Scotland
- the policies and practices of criminal justice bodies in relation to forensic information (eg reviewing practices in relation to taking forensic information from children in relation to less serious offences)

---

15 The review did not, given that the Scottish Government had rejected the option, consider the possibility of permanently retaining forensic information from people who are not convicted (Fraser 2008, p 13).
16 The recommendations are set out at pages 19 and 20 of the Fraser Report.
• changes to the law so that the rules for taking and retaining fingerprint data from people who are prosecuted in the criminal courts for relevant sexual or violent offences are the same as those for DNA data

• changes to the law so that the rules for taking and retaining fingerprint and DNA data from children who are dealt with through the children’s hearings system, and either accept that they have committed a relevant sexual or violent offence or are found to have done so by a sheriff, are the same as those for people convicted of an offence in the criminal courts.

At the same time as publishing the Fraser Report, the Scottish Government issued its own consultation paper in relation to the issues raised by the report – Fraser Report on Retention of DNA and Fingerprint Data – Government’s Response (Scottish Government 2008b) (“the Government Consultation Paper”). Responses to the Government Consultation Paper are also available online (Scottish Government 2009a).

The Bill

The Criminal Justice and Licensing (Scotland) Bill [as introduced] (‘the Bill’) includes a number of provisions which are intended to:

“enhance public protection and improve the law in relation to the retention and use of DNA, fingerprints and other physical data”. (Policy Memorandum, para 293)

The Policy Memorandum published along with the Bill goes on to state that, in putting forward proposals for change, the Scottish Government wants to ensure that the rules in this area maintain a proper balance between: (a) the benefits to law enforcement of retaining forensic information; and (b) the civil liberty implications of retaining such information (particularly DNA data) obtained from people who are not convicted of an offence. In this context, the Policy Memorandum makes it clear that the intention of the Scottish Government is that there should be no change to the current rules under which the police have the power to keep fingerprint and DNA data indefinitely only where a person is convicted in the criminal courts.

In relation to the retention of fingerprint and DNA data, sections 58 to 60 of the Bill would amend the current provisions of the Criminal Procedure (Scotland) Act 1995 in the following ways:

1. Extended retention powers where a suspect is prosecuted in the criminal courts for a relevant sexual or violent offence but not convicted

The extended police retention powers currently applying to DNA data (introduced by provisions in the Police, Public Order and Criminal Justice (Scotland) Act 2006) were outlined earlier in this briefing. Section 58 of the Bill seeks to apply these extended retention powers to fingerprint data (and various other types of print such as palm prints).

2. Retention of fingerprint and DNA data obtained from children who are dealt with by way of the children’s hearings system after committing sexual or violent offences

Section 59 of the Bill provides for extended police retention powers, in relation to both fingerprint and DNA data, obtained from children who are dealt with through the children’s hearings system. At present such data should be deleted as soon as possible following a decision not to prosecute a child in the criminal courts. Thus, a decision to deal with a child through the

---

17 In relation to relevant violent offences, this recommendation excluded less serious assaults.
18 Paragraphs 8.1 to 8.5 of the Government Consultation Paper set out the options put forward by the Scottish Government.
children’s hearings system should lead to deletion. The provisions in the Bill would allow the police to retain such data where a child is referred to a children’s hearing and either: (a) accepts that he/she has committed a ‘relevant offence’; or (b) is held by a sheriff to have committed a ‘relevant offence’. The Bill would give the Scottish Ministers the power to provide, by way of statutory instrument, that some or all of the relevant sexual and violent offences set out in section 19A(6) of the Criminal Procedure (Scotland) Act 1995 are also ‘relevant offences’ for the purposes of these new provisions. The Policy Memorandum indicates that the “list of applicable violent and sexual offences would be developed in consultation with interested parties” (para 302). A Scottish Government (2009b) news release indicated that the Government intends to establish an expert working group and that the remit of the group will include overseeing the development of a list of applicable offences.

The extended retention powers would not allow for the indefinite retention of fingerprint and DNA data. Instead, the Bill provides for a three year retention period with the possibility of extension on application by a chief constable to a sheriff. Thus, the rules governing the period of retention would be very similar to those which currently exist in relation to DNA data obtained from a suspect who is prosecuted in the criminal courts for a relevant sexual or violent offence but not convicted. It may be noted that the Bill departs from the recommendations of the Fraser Report in this respect. The Fraser Report recommended indefinite retention where a child has committed a serious sexual or violent offence and is dealt with through the children’s hearings system (ie retention in line with the rules governing people who are convicted of an offence in the criminal courts).

3. Purposes for which fingerprint and DNA data can be used

Section 60 of the Bill contains provisions setting out the general purposes for which fingerprint and DNA data obtained by the police can be used. It provides that such information may be used for: (a) the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution; or (b) the identification of a deceased person or a person from whom the information came.

The Explanatory Notes published along with the Bill state that the police currently rely on common law powers relating to the use of fingerprint and DNA data. The statutory provisions are intended to provide greater clarity in relation to police powers, without interfering with any existing powers.

Retention of Data and Alternatives to Prosecution

The Government Consultation Paper also sought views on proposals to change the rules for retaining/destroying fingerprint and DNA data where a case is concluded by an alleged offender accepting a prosecution offer of a direct measure (eg a fiscal fine) as an alternative to prosecution in the criminal courts. At present, fingerprint and DNA data must be destroyed in such circumstances. The consultation paper sought views on two proposals:

“DNA and fingerprint samples taken from persons arrested or detained on suspicion of having committed an offence and who subsequently accept an offer by the procurator fiscal of a fiscal fine, compensation order, combined order or work order should be retained indefinitely, in the same way as they are in respect of persons convicted of an offence; or alternatively

DNA and fingerprint samples taken from persons arrested or detained on suspicion of having committed an offence and who subsequently accept an offer by the procurator fiscal of a fiscal fine, compensation order, combined order or work order should be retained for a period of 3 years, with discretion for a chief constable to apply to a
sheriff for an extension of up to 2 years at the end of that period.” (Scottish Government 2008b, para 6.5)

Consultation responses expressing support for one of the above options included:

- in support of the first option of indefinite retention – Association of Chief Police Officers in Scotland; Scottish Police Authorities Conveners Forum; and Scottish Police Federation; Scottish Police Services Authority
- in support of the second option of time limited retention – Faculty of Advocates; and Information Commissioner’s Office

Consultation responses raising possible concerns about either option included those from the Human Genetics Commission and the Law Society of Scotland.

The Bill as introduced does not contain provisions on this issue. A Scottish Government (2009b) news release stated that:

“Responses to a Scottish Government consultation were divided on whether forensic data obtained from people who subsequently accept direct measures issued by procurators fiscal should be retained – whether temporarily or indefinitely.

The Association of Chief Police Officers in Scotland and the Scottish Police Services Authority also called for the retention of forensic data taken from individuals who subsequently accept a police fixed penalty notice.

Mr MacAskill said: 'Recent reforms to the summary justice system mean that cases of less serious but nonetheless criminal activity that were previously prosecuted through the courts are being dealt with more swiftly through fiscal direct measures or, for lower level offending, police fixed penalty notices. We want to consider carefully, working with Parliament, whether forensic data in such cases should also be retained and, if so, for how long’.”
SOURCES


Scottish Parliament Information Centre (SPICe) Briefings are compiled for the benefit of the Members of the Parliament and their personal staff. Authors are available to discuss the contents of these papers with MSPs and their staff who should contact Frazer McCallum on extension 85189 or email frazer.mccallum@scottish.parliament.uk. Members of the public or external organisations may comment on this briefing by emailing us at spice@scottish.parliament.uk. However, researchers are unable to enter into personal discussion in relation to SPICe Briefing Papers. If you have any general questions about the work of the Parliament you can email the Parliament’s Public Information Service at sp.info@scottish.parliament.uk.

Every effort is made to ensure that the information contained in SPICe briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.