HOUSE OF COMMONS
LIBRARY

Protection of Freedoms Bill

Bill 146 of 2010-11

RESEARCH PAPER 11/20 23 February 2011

This briefing on the *Protection of Freedoms Bill* has been prepared for the Second Reading debate on the Bill in the House of Commons. This is due to take place on 1 March 2011.

The Bill would bring in a new framework for police retention of fingerprints and DNA data, and require schools to get parents' consent before processing children's biometric information. It would introduce a code of practice for surveillance camera systems and provide for judicial approval of certain surveillance activities by local authorities. Another code of practice would cover officials' powers of entry, and these powers would be subject to review and repeal. The Bill would outlaw wheel-clamping on private land.

There would be new regime for police stops and searches under the *Terrorism Act 2000* and the Bill would reduce the maximum pre-charge detention period under that Act from 28 to 14 days. It would restrict the scope of the "vetting and barring" scheme to protect vulnerable groups and make changes to criminal records checks. Those with convictions for consensual sexual relations between men aged 16 or over (which have since been decriminalised) would be able to apply to have them disregarded.

The Bill would extend Freedom of Information rights by requiring datasets to be available in a re-usable format. It would repeal provisions (never brought into force) which would have allowed trial without a jury in complex fraud cases, and remove time restrictions for marriage or civil partnership.

Sally Almandras

Recent Research Papers

11/10	UK Defence and Security Policy: A New Approach?	21.01.11
11/11	Health and Social Care Bill [Bill 132 of 2010-11]	27.01.11
11/12	Economic Indicators, February 2011	01.02.11
11/13	Anonymity (Arrested Persons) Bill [Bill 9 of 2010-11]	02.02.11
11/14	Education Bill [Bill 137 of 2010-11]	03.02.11
11/15	Budget Responsibility and National Audit Bill [HL] [Bill 143 of 2010-11]	08.02.11
11/16	The Local Government Finance Settlement 2011-13	08.02.11
11/17	Legislation (Territorial Extent) Bill [Bill 10 of 2010-11]	08.02.11
11/18	Wash-up 2010	11.02.11
11/19	Unemployment by Constituency, February 2011	16.02.11

Research Paper 11/20

Contributing Authors: Sally Almandras: DNA retention, criminal records, fraud
Christine Gillie: Biometric information in schools
Alexander Horne: Pre-charge detention
Pat Strickland: Powers of entry, s44 stops and searches
Grahame Danby: Surveillance
Louise Butcher: Wheel-clamping, parking
Oonagh Gay: Freedom of Information
Catherine Fairbairn: Marriage and civil partnership
Gavin Berman: Statistics

ISSN 1368-8456

Contents

Summary

The Coalition Government promised to introduce a "Freedom Bill" in its Programme for Government. It conducted an online consultation, inviting the public to suggest laws they felt should be changed; there is also to be a pilot "public reading stage" during which comments from the public will be considered.

Part 1 of the Bill would introduce a new framework for the retention of fingerprints and biometric data taken from arrested or convicted people, based largely on the Scottish system. The current law permits indefinite retention of such data, but this has been ruled unlawful by the European Court of Human Rights. The Bill would introduce a new regime based on the presumption that data should be destroyed unless circumstances permitting its retention apply. The main change would be that data from people arrested but not convicted would have to be deleted, unless the offence was a specified serious one in which case the data could be retained for up the three years (plus a single two year extension if thought necessary).

Chapter 2 of Part 1 would require schools and further education institutions to obtain the written consent of parents before processing biometric information from children under the age of 18. Examples include fingerprint identification for purposes such as registration or cashless canteens. This follows concern in some quarters about the use of such information.

Part 2 of the Bill is concerned with the regulation of surveillance. Chapter 1 makes provision for the Secretary of State to prepare a code of practice for surveillance camera systems, including CCTV and Automatic Number Plate Recognition systems. This code will be overseen by a new Surveillance Camera Commissioner. Chapter 2 provides for judicial approval of those types of surveillance which are available to local authorities under the *Regulation of Investigatory Powers Act 2000*. The relevant surveillance activities are access to communications data and the use of directed surveillance and covert human intelligence sources (undercover agents).

Chapter 1 of Part 3 deals with statutory powers of entry. Over 1,200 powers have been introduced over decades allowing officials to enter property without the owner's permission. There is little consistency about warrants, the use of force or the penalty for obstruction. Some argue that the combined effect makes it impossible for ordinary people to be aware of their rights. Following a Home Office review started by the previous Government, the Bill would repeal some of the powers and require ministers to review others. Further repeals, consolidations and safeguards could be made by order, and the Bill would introduce a code of practice.

Chapter 2 of Part 3 would outlaw the clamping of vehicles on private land and abolishes the previous Government's licensing scheme for companies that undertake clamping work as it will no longer be necessary. The Bill provides that in certain circumstances, private landowners will be able to enforce parking tickets on their land against the 'keeper' or owner of a vehicle, even when they are not the driver.

Part 4 of the Bill makes changes to certain counter-terrorism powers introduced by the *Terrorism Act 2000* (as amended). These moves were heralded by the Government's Review of Counter-Terrorism and Security Powers, which reported in January 2011. It repeals controversial provisions for stopping and searching people without "reasonable suspicion" under sections 44-47 of the *Terrorism Act 2000*. This, too, was in response to an adverse judgement by European Court of Human Rights. The Bill replaces these powers with a more limited regime. The police will still be able to authorise areas for stopping and searching people without "reasonable suspicion", but only when a senior officer reasonably expects an act of terrorism will take place. The purposes of the search are more tightly drawn and the

period of authorisation is halved, although it could still be renewed. Both the period of authorisation and the area would have to be no greater than necessary.

Part 4 would also ensure a permanent reduction of the maximum period of pre-charge detention to 14 days. This proposal has been coupled with the publication of draft emergency legislation that could be introduced in "exceptional circumstances." If introduced, this legislation would have the effect of re-introducing 28 day pre-charge detention for a fixed period of three months. It would undergo pre-legislative scrutiny. Separate legislation, expected to bring an end to the use of control orders, is due to be published shortly.

Part 5 of the Bill deals with safeguarding vulnerable groups and criminal records. Chapter 1 would make a number of changes aimed at restricting the scope of the vetting and barring scheme established by the *Safeguarding Vulnerable Groups Act 2006*. The "vetting" element of the scheme, which would have required people wanting to work with children or vulnerable adults to go on a register and be monitored, would be scrapped. The "barring" element of the scheme, which prevents unsuitable people from undertaking such work, would continue but with a more limited scope.

Chapter 2 of Part 5 proposes several changes to the current system for criminal records checks. The changes are based on recommendations made by Sunita Mason, the Government's Independent Advisor for Criminality Information Management. The changes would include an end to the practice of sending the results of a criminal records check directly to employers, tightening up the test used by the police when deciding whether to disclose non-conviction information, and introducing a new procedure for the continuous updating of criminal records certificates.

Chapter 3 of Part 5 would enable men with convictions under sections 12 (buggery) and 13 (gross indecency between men) of the *Sexual Offences Act 1956* to apply to the Home Secretary to have the convictions disregarded. To fall within the scheme, the convictions would have to have been for conduct that has since been decriminalised: namely consensual sexual relations between men aged 16 or over. Disregarded convictions would not need to be disclosed to prospective employers.

Part 6 of the Bill would extend Freedom of Information rights by requiring datasets to be available in a re-usable format. It would also give the Information Commissioner more independence in terms of hiring staff and protection against dismissal.

Clause 99 of the Bill would repeal section 43 of the *Criminal Justice Act 2003*, which would have enabled the prosecution in certain serious and complex fraud cases to apply for the trial to be conducted without a jury. Section 43 has never been brought into force.

Clause 100 of the Bill would remove the time restrictions for marriage or civil partnership and the associated offences in England and Wales. This would mean, effectively, that either could take place at any time of the day or night (subject to there being someone available to officiate).

1 Introduction

1.1 Overview

The *Protection of Freedoms Bill* was introduced in the House of Commons on 11 February 2011 as Bill 146 of 2010-11. Information on the Bill and its progress is available from the *Protection of Freedoms Bill 2010-11* page of the Parliament website.

The introduction of a "Freedom Bill" was a commitment originally made in the Government's *The Coalition: our programme for government* ("the Coalition Programme"), published on 20 May 2010. This argued that:

> the British state has become too authoritarian, and that over the past decade it has abused and eroded fundamental human freedoms and historic civil liberties. We need to restore the rights of individuals in the face of encroaching state power, in keeping with Britain's tradition of freedom and fairness.[1]

The Programme went on to say that the Government would "implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion".[2] In addition to a Freedom Bill, these measures would include the abolition of identity cards, and specific commitments in a number of areas.[3]

The *Identity Documents Act 2010* has since abolished identity cards; further background can be found in Library Research Paper 10/41, *Identity Documents Bill*, 4 June 2010.

The *Protection of Freedoms Bill* is, according to the Government, the "next step" in its legislative programme to safeguard civil liberties.[4] To assist with the drafting of the Bill, a 'Your Freedom' online consultation invited the public to suggest laws and regulations that they felt should be changed. When the website closed on 10 September 2010, 47,212 people had registered as users, with 15,238 ideas having been submitted and 76,994 comments posted.[5] These can be viewed on an archived version of the website. The Government stated that all suggestions would be taken into account.[6]

The Home Office summarises the Bill's provisions as follows:

- adopting the protections of the Scottish model for the retention of DNA and fingerprints
- introducing a requirement for schools and colleges to obtain the consent of parents before taking fingerprints and other biometric data from children under the age of 18 years
- introducing a code of practice for closed circuit television and other surveillance camera systems and the appointment of a surveillance camera commissioner
- safeguarding against the misuse of counter-terrorism and security powers, in particular, the use of the Regulation of Investigatory Powers Act 2000 by local authorities, stop and search powers, and pre-charge detention

---

1 HM Government, *The Coalition: our programme for Government*, May 2010, p11
2 Ibid
3 See p11 of the *Coalition Programme* for further detail
4 Home Office website, *Protection of Freedoms Bill*, [on 18 February 2011]
5 HL Deb 7 October 2010 cc29-30WA
6 HL Deb 7 October 2010 c30WA

- repealing unnecessary powers of entry, consolidating other existing powers of entry, and attaching additional safeguards to their use
- creating a new criminal offence of immobilising, moving or preventing the movement of a vehicle without lawful authority
- reforming the vetting and barring scheme and criminal records regime
- changing the law so that historical convictions for consensual gay sex with over-16s no longer have to be disclosed
- extending the freedom of information regime to cover companies wholly owned by two or more public authorities
- creating an obligation on departments and other public authorities to proactively release datasets in a reusable format
- changing the appointment and accountability arrangements to enhance the independence of the Information Commission
- repealing provisions removing the right to trial by jury in serious fraud trials[7]

This Research Paper deals with each subject in the order in which the relevant provisions occur in the Bill.

The Coalition Agreement included a commitment to introduce a 'public readings stage' whilst Parliament was considering legislation:

> We will introduce a new 'public reading stage' for bills to give the public an opportunity to comment on proposed legislation online, and a dedicated 'public reading day' within a bill's committee stage where those comments will be debated by the committee scrutinising the bill.[8]

On 15 February 2011, the Deputy Prime Minister, Nick Clegg, announced that the Government was "launching a website (www.publicreadingstage.cabinetoffice.gov.uk) that will allow the public to comment on the *Protection of Freedoms Bill* online, before the House of Commons commences its considerations at Second Reading". The public had been asked to generate ideas for inclusion in the Bill before it was published and this process meant that the public's involvement could be maintained. The Deputy Prime Minister said that the public reading stage of the *Protection of Freedoms Bill* was a pilot scheme to allow technology to be tested and that no changes to the House's procedures would be required.[9]

The deadline for comments is 7 March 2011.[10]

The Government will collate the comments and present them to the public bill committee established to scrutinise the Bill.[11]

---

7 Home Office website, *Protection of Freedoms Bill* [on14 February 2011]
8 HM Government, *The Coalition: our programme for government*, May 2010, p27
9 HC Deb 15 February 2011 c73WS
10 *Protection of Freedoms Bill – Public Reading Stage*, "What is a Public Reading Stage?"
11 Cabinet Office, *Big Society: Opening Up Parliament to the People*, 15 February 2011

1.2 Territorial extent

The majority of the Bill extends to England and Wales only. However certain provisions also extend to Scotland and Northern Ireland; these are set out in **clause 105** and are summarised in paragraphs 69 to 76 of the Explanatory Notes to the Bill.

Scotland

The provisions which extend to Scotland relate to reserved matters and are as follows: the retention of fingerprints and DNA profiles (clauses 19 to 22 and parts 1 to 5 of Schedule 1); the requirement for local authorities to obtain judicial approval for the application and use of communications data under the *Regulation of Investigatory Powers Act 2000* (chapter 2 of part 2); certain powers of entry (chapter 1 of part 3); repeal of the order-making power in the *Terrorism Act 2006* relating to pre-charge detention (clause 57); changes to terrorism stop and search powers (clauses 58 to 61); amendments to the *Freedom of Information Act 2000* and the *Data Protection Act 1998*.

The Bill does not contain any provisions falling within the terms of the Sewel Convention. However if there are amendments relating to devolved matters in Scotland, the consent of the Scottish Parliament will be sought for them.

Wales

Most of the Bill would apply to Wales. However some of the Bill's provisions relate to devolved matters or confer functions on the Welsh Ministers. They will therefore require the National Assembly of Wales to pass a legislative consent motion, or the consent of Welsh Ministers. These provisions relate to: the requirement to obtain parental consent before processing a child's biometric information in schools (chapter 2 of part 1); powers of entry (chapter 1 of part 3); making the keeper of a vehicle responsible, in certain circumstances, for unpaid parking charges (clause 56); amendments to the *Safeguarding Vulnerable Groups Act 2006* (chapter 1 of part 5).

Northern Ireland

The provisions of the Bill relating to the following excepted or reserved matters also extend to Northern Ireland: the retention of fingerprints and DNA profiles (clauses 19 to 22 and parts 1 to 3 and 6 of Schedule 1); the requirement for local authorities to obtain judicial approval for the application and use of covert surveillance powers under the *Regulation of Investigatory Powers Act 2000* (chapter 2 of part 2); certain powers of entry (chapter 1 of part 3); repeal of the order-making power in the *Terrorism Act 2006* relating to pre-charge detention (clause 57); changes to terrorism stop and search powers (part 4); amendments to the *Data Protection Act 1998.*

The provisions of the Bill amending the *Freedom of Information Act 2000* (clauses 93 to 96 and 98) also extend to Northern Ireland. As these relate to transferred matters, they will require the consent of the Northern Ireland Assembly (NIA). If amendments are made to the Bill that trigger a further requirement for a legislative consent motion, the consent of the NIA will be sought.

2 The retention of fingerprint and DNA data

2.1 The current law

Sections 61 to 65 of the *Police and Criminal Evidence Act 1984* (PACE) set out the current law on the taking, retention, use and destruction of fingerprints and biometric samples. The *Terrorism Act 2000* makes similar provisions in respect of biometric data from people being detained under that Act.

PACE

The general rule under PACE is that the police may not take fingerprints or a non-intimate sample[12] from a person without his consent. However, there are a number of exceptions to this rule, in which case the police can take fingerprints or non-intimate samples **without** consent. The most important of these exceptions are where a person has been arrested for, charged with or convicted of a recordable offence.[13]

Section 64 of PACE permits fingerprints or samples taken from a person in connection with an offence to be retained after they have fulfilled the purposes for which they were taken. However, they may not be used other than for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution, the identification of a deceased person or of the person from whom a body part came, or (in respect of samples from persons subject to a control order) in the interests of national security.[14]

While section 64 of PACE permits the retention of samples, it does not currently specify any time limits for such retention or any procedure by which samples can be removed. Instead, time limits and a removal procedure (known as the "exceptional case procedure") are set out in non-statutory guidance issued by the Association of Chief Police Officers (ACPO). The guidance states that an individual's record on the Police National Computer (including fingerprints and samples) will be retained until that person is deemed to have attained 100 years of age.[15] A record may be removed prior to this date only 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.
>
> (...)
>
> 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.[16]

The Terrorism Act 2000

Schedule 8 to the *Terrorism Act 2000* contains similar provisions to PACE in respect of fingerprints and samples from individuals detained under Schedule 7 or section 41 of the 2000 Act. Fingerprints or non-intimate samples may only be taken from such a person either with his consent, or without consent where either of the following two conditions is satisfied:

- he is detained at a police station and a police officer of at least the rank of superintendant authorises the fingerprints/sample to be taken; or

---

12 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))

13 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).

14 PACE, s64(1A)-(1AB)

15 ACPO, *Retention Guidelines for Nominal Records on the Police National Computer*, March 2006, para 3.1

16 Ibid, Appendix 2

- he has been convicted of a recordable offence and, where a non-intimate sample is to be taken, he was convicted of the offence on or after 10 April 1995 (29 July 1996 where the sample is to be taken in Northern Ireland).

Fingerprints and samples taken under the provisions in Schedule 8 may be retained indefinitely, but may only be used for the purposes of a terrorist investigation, for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution, or in the interests of national security.

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.

2.2 *S and Marper*: the European Court of Human Rights

Two individuals from whom fingerprints and samples had been taken, S (an 11 year old acquitted of robbery) and Marper (a man against whom proceedings for harassment of his partner had been discontinued), brought court proceedings challenging the indefinite retention of their data by the police on the grounds that this was incompatible with Article 8 of the European Convention on Human Rights (ECHR).

Proceedings before the domestic courts were unsuccessful,[17] but S and Marper went on to appeal to the European Court of Human Rights. Judgment was handed down on 4 December 2008, with the Court ruling in S and Marper's favour.[18] The Court accepted that the retention of fingerprint and DNA information pursued a legitimate purpose, namely the detection and prevention of crime. However, it went on to unanimously hold that the retention and storage of the applicants' fingerprints and DNA samples was disproportionate and not "necessary" in a democratic society, and therefore violated Article 8. The Court said:

> 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; 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.

2.3 The position in Scotland

Scotland has a different system for the retention of fingerprints and DNA data, to which the European Court of Human Rights drew specific attention in its judgment:

---

17 [2002] EWHC 478 (Admin) (High Court), [2002] EWCA Civ 1275 (Court of Appeal), [2004] UKHL 39 (House of Lords). A more detailed overview of the domestic proceedings is set out in Library Standard Note SN/HA/4049 *Retention of fingerprints and DNA data*.

18 *Case of S. And Marper v The United Kingdom*, Applications nos. 30562/04 and 30566/04. Press release 880 issued by the Registrar on 4 December 2008 provides an overview of the case.

Scotland

> 36. Under the 1995 Criminal Procedure Act of Scotland, as subsequently amended, the DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. A recent qualification provides that biological samples and profiles may be retained for three years, if the arrestee is suspected of certain sexual or violent offences even if a person is not convicted (section 83 of the 2006 Act, adding section 18A to the 1995 Act.). Thereafter, samples and information are required to be destroyed unless a Chief Constable applies to a Sheriff for a two-year extension.
>
> (...)
>
> 109. The current position of Scotland, as a part of the United Kingdom itself, is of particular significance in this regard. As noted above (see paragraph 36), 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. [19]

The Court went on to state that the Scottish position was:

> ...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 (see paragraphs 43-44 above).[20]

More detailed guidance on the Scottish system is available in a briefing note prepared by the Scottish Parliament Information Centre.[21]

2.4 The *Crime and Security Act 2010*

The Labour Government's response to the S and Marper decision came in the form of the *Crime and Security Act 2010*, which received Royal Assent on 8 April 2010. Detailed background to the 2010 Act is set out in Library Standard Note SN/HA/4049 *Retention of fingerprint and DNA data* (pp6-11), Library Research Papers 09/97 *Crime and Security Bill* (pp12-23) and 10/22 *Crime and Security Bill: Committee Stage Report* (pp3-12), and in the Lords Library Note 2010/010 *Crime and Security Bill* (pp4-10).

Section 14 of the 2010 Act would have amended section 64 of PACE to introduce the following more restricted regime for the retention of fingerprints and biometric data:

> The retention periods for the various categories of data depend on a number of factors including the age of the individual concerned, the seriousness of the offence or alleged offence, whether the individual has been convicted, and if so whether it is a first conviction. The different categories can be summarised as follows:
>
> - Adults - convicted: indefinite retention of fingerprints, impressions of footwear and DNA profile (see substituted section 64(2));
>
> - Adults - arrested but unconvicted: retention of fingerprints, impressions of footwear and DNA profile for 6 years (see new section 64ZD);

---

19 Ibid, paras 36 and 109
20 Ibid, para 110
21 Scottish Parliament Information Centre Briefing 09/30, *Criminal Justice and Licensing (Scotland) Bill: Fingerprint and DNA Data*, 1 May 2009

- Under 18 year olds - convicted of serious offence or more than one minor offence: indefinite retention of fingerprints, impressions of footwear and DNA profile (see substituted section 64(2));

- Under 18 year olds - convicted of single minor offence: retention of fingerprints, impressions of footwear and DNA profile for 5 years (see new section 64ZH);

- 16 and 17 year olds - arrested for but unconvicted of serious offence: retention of fingerprints, impressions of footwear and DNA profile for 6 years (see new section 64ZG);

- All other under 18 year olds - arrested but unconvicted: retention of fingerprints, impressions of footwear and DNA profile for 3 years (see new sections 64ZE and 64ZF);

- Persons subject to a control order: retention of fingerprints and DNA profile for 2 years after the control order ceases to have effect (see new section 64ZC);

- All DNA samples: retained until profile loaded onto database, but no more than 6 months (see new section 64ZA).[22]

However, the 2010 general election followed shortly after the Act was passed and section 14 has therefore never been commenced.

2.5 The Government's proposals for change

During the 2010 Act's passage through Parliament, both the Conservatives and the Liberal Democrats argued that its provisions did not go far enough and voted against the relevant clauses in Committee.[23] During the Bill's final stages in the Lords, the Liberal Democrats tabled an amendment that would have replaced the Labour Government's proposals with a more limited retention framework. However, the Conservatives unexpectedly allowed the DNA provisions through unamended. Baroness Neville-Jones emphasised that this was because it was important to enshrine the concept of limited retention in law sooner rather than later, even if the retention periods were longer than the Conservatives agreed with:

> Systematic reform is needed and a new approach focused on the guilty and on those who pose most risk. This is a fundamental root and branch change that we will not achieve today but which must be achieved by a new Government. For now, we take the view that it is important that we have in law acceptance of the proposition that the indefinite retention of innocent people's DNA is unacceptable and illegal.[24]

Following the 2010 election, the Government indicated that it would be legislating to "adopt the protections of the Scottish model for the DNA database".[25]

2.6 The Bill's provisions

The Bill would repeal section 14 of the *Crime and Security Act 2010* without it ever having been brought into force. Section 64 of PACE, which currently provides for the retention of fingerprints and biometric samples after they have fulfilled the purposes for which they were taken, would also be repealed. The Bill would introduce a new retention model based largely

---

22 Explanatory Notes to the *Crime and Security Act 2010*, para 51
23 See Library Research Paper 10/22 *Crime and Security Bill: Committee Stage Report*, pp5-8
24 HL Deb 7 April 2010 cc1150-1151
25 HM Government, *The Coalition: our programme for government*, May 2010, p11

on the Scottish system described above.[26] The Explanatory Notes to the Bill include a table comparing the current section 64 rules, the rules that section 14 would have introduced, the position in Scotland and the proposed changes under the Bill. This is reproduced at Appendix 1 of this research paper. Analysis of some of the Bill's key clauses is set out below.

Clause 1 of the Bill would insert a new section 63D into PACE, under which there would be a general presumption that fingerprints and DNA profiles (referred to in the Bill as "section 63D material") would **have** to be destroyed unless one or more of new sections 63E to 63N applied.[27] The police would retain the power to carry out a speculative search against the fingerprints and/or biometric data before destroying them.

New section 63E, inserted by **clause 2**, would permit the retention of section 63D material taken from a person in connection with the investigation of an offence until either the conclusion of the police investigation or the conclusion of any related criminal proceedings brought against that person.

Clause 3 covers the retention of section 63D material taken from persons arrested for or charged with, but not convicted of, certain violent, sexual and terrorist offences referred to as "qualifying offences".[28] Under new section 63F, the following retention regime would apply:

- if the person arrested for or charged with a qualifying offence had a previous conviction for a recordable offence,[29] his section 63D material could be retained indefinitely;
- if the person was charged with a qualifying offence (but not convicted) and had no previous convictions, his section 63D material could be retained for three years; and
- if the person was arrested for a qualifying offence (but not charged or convicted) and had no previous convictions, his section 63D material could be retained for three years if one or more circumstances to be prescribed by the Secretary of State applied.[30]

The police would be able to apply to the magistrates' courts for a single two year extension in respect of section 63D material subject to an initial three year retention period. The police would 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 would have a similar right of appeal against a decision to permit an extension.

Clause 4 would require section 63D material from a person arrested for or charged with (but not convicted of) a minor offence to be destroyed, unless the person had a previous conviction for another recordable offence,[31] in which case the material could be retained indefinitely.

---

26 For some of the key differences between the Bill and the Scottish system, see *Protection of Freedoms Bill, European Convention on Human Rights – Memorandum by the Home Office*, February 2011, paras 16-21

27 In cases where more than one of the new sections applied, the longest retention period available would be used.

28 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 has not yet been brought into force.

29 Other than an "excluded offence": namely a conviction for a minor offence committed when the person was under 18 and for which a sentence of less than five years' imprisonment was imposed (new section 63F(13)).

30 New section 63F(11) would require one such circumstance to be that the proposed new Commissioner for the Retention and Use of Biometric Material (see **clause 20**) had consented to the retention of the material concerned. The Secretary of State's order setting out the prescribed circumstances would be subject to the affirmative resolution procedure.

31 Again, other than an "excluded offence": new section 63G(3) (see footnote 16)

Under new section 63H, inserted by **clause 5**, material from adults convicted of a recordable offence or under 18s convicted of a qualifying offence would be retained indefinitely (as is the case now).[32]

The retention of material from under 18s convicted of a first minor offence (ie a recordable offence other than a qualifying offence) would be determined by reference to the length and nature of the sentence imposed. **Clause 7** would provide for indefinite retention where a custodial sentence of five or more years was imposed. For a custodial sentence of less than five years, the retention period would be the duration of the sentence plus a further five years. For non-custodial sentences, the retention period would be five years from the date on which the material was taken. A subsequent conviction for a further recordable offence (whether before or after the individual's 18th birthday) would enable the material to be retained indefinitely.

Clause 9 would give chief constables the power to determine that material that would otherwise have to be destroyed should be retained on national security grounds. Any such "national security determination" would be valid for up to two years, and the chief constable would be able to extend it for further two year periods. National security determinations would be subject to review by a new Commissioner for the Retention and Use of Biometric Material, a position that would be established under **clause 20**. Chief constables making national security determinations would have to notify the Commissioner of any determination made, including a statement of the reasons why it was made and any supporting documentation. The Commissioner would have the power to overturn the determination and order the destruction of the material. There would be no appeal against the Commissioner's decisions other than by way of judicial review. **Clause 22** would require the Secretary of State to issue guidance on the making and renewal of national security determinations. Such guidance would require Parliamentary approval via affirmative resolution.

Material given voluntarily would have to be destroyed as soon as it had fulfilled the purpose for which it was taken (**clause 10**).

All of the destruction provisions outlined above could be overridden if the person from whom the material was taken consented in writing to its retention (**clause 11**). Consent could be withdrawn at any time.

Physical samples from which DNA profiles are derived (e.g. saliva or hair samples) would have to be destroyed as soon as a DNA profile was satisfactorily derived from them, and in any event within six months of the taking of the sample (**clause 14**).

Part 1 of Schedule 1 would introduce a broadly equivalent regime for material taken under the *Terrorism Act 2000* as opposed to PACE. Material taken from a person detained under section 41 or Schedule 7 of the 2000 Act could be retained indefinitely where that person had a previous conviction for a recordable offence. Material from a person with no previous convictions detained under section 41 could be retained for a three year period, with the possibility of extension for further periods of up to two years at a time.[33] Material from a person with no previous convictions detained under Schedule 7 would have to be deleted within six months. The police would have the power to make national security determinations authorising the retention of material beyond these limits. Again, the exercise of this power would be subject to review by the Commissioner.

Clause 25 would require the Secretary of State to make regulations (subject to the negative resolution procedure) prescribing the framework for retaining and destroying fingerprints and

---

[32] See **clause 7** for the proposed rules regarding under 18s convicted of minor offences

[33] This differs from the PACE proposals in **clause 3**, which would only permit a single two year extension.

biometric material that has already been taken at the time the Bill's provisions come into force. It is intended that these regulations would apply the new framework set out in the Bill to existing biometric material.[34]

The Home Office has described the Bill's proposals as "more readily justifiable in ECHR terms than those of the Crime and Security Act 2010".[35] GeneWatch UK, a campaign group that monitors genetic technologies, has said that it "broadly welcomes" the Bill's provisions.[36] However, shadow home secretary Yvette Cooper has said that the Government is "going too far on DNA retention and ... going against the evidence that shows it has a significant impact bringing serious criminals to justice and exonerating innocent people".[37]

3 Biometric information of children in schools and colleges

3.1 Background

Biometric identification systems are used in some schools for practical purposes such as registration, cashless canteens and library book borrowing. The most common biometric system used in schools is the automated fingerprint identification system; however, a small number of schools have used other biometric systems such as iris, face or palm recognition technology. There are no official figures on how many schools use biometric systems but there are estimates that 30% of secondary schools and 5% of primary schools use them. There is also no official evidence concerning pupils' and parents' views on the use of biometric systems in schools although there are indications that many parents oppose the practice.[38]

In an adjournment debate on 23 July 2007, Greg Mulholland raised the issue, stressing that many parents were often not asked for their consent and in many cases were not even informed. He said that there was real concern from parents and civil liberties organisations. Responding, Jim Knight, then Minister for Schools, announced the publication of guidance drawn up by the British Education Communications and Technology Agency (Becta) on behalf of the then Department for Children, Schools and Families (DCSF).[39]

While noting the powers[40] schools have to run themselves efficiently, the Becta guidance advised schools to involve parents fully in any decision to introduce a biometric system, including how the technology would be used, what data would be held and how it would be stored etc. Becta also advised that schools should recognise some parents' and pupils' concerns and offer alternative systems to access the same services. The guidance set out how the *Data Protection Act 1998* (DPA) applied to the use of biometric data in schools, and included the eight data protection principles with which data controllers must comply. The guidance also noted other legal considerations that apply to the collection of data more generally, such as the *Human Rights Act 1998*.[41]

The Information Commissioner's Office (ICO) also issued guidance on the use of biometrics in schools. The ICO commented on the use of fingerprint images, the storage of information, and the issue of parental consent. It noted that for the purposes of the DPA the pupils

---

34 *Protection of Freedoms Bill, Explanatory Notes, Bill 146-EN*, paragraph 124, and **clause 25(3)**

35 Home Office, *Protection Of Freedoms Bill, European Convention On Human Rights – Memorandum By The Home Office*, February 2011, para 14

36 GeneWatch UK website, *Freedom Bill* [on 16 February 2011]

37 "DNA profiles to be deleted from police database", *BBC News website*, 11 February 2011

38 Department for Education, *Protection of Freedoms Bill*, *Impact assessment: biometrics in schools and introduction of parental consent*, p6; "Europe tells Britain to justify itself over fingerprinting children in schools", *Telegraph*, 14 December 2010

39 HC Deb 23 July 2007 cc659-666; HC Deb 23 July 2007 cc41-2WS

40 *Education Act 2002*, Schedule 1, paragraph 3(1)

41 *Becta guidance on biometric technologies in schools*, July 2007

themselves are "data subjects", and that it is they who should in the first instance be informed and consulted about the use of their personal data. Deciding when children are mature enough to decide such matters may be difficult. The guidance said that while there is nothing explicit in the Act to require schools to seek consent from all parents before implementing a fingerprinting application, unless schools can be certain that all children understand the implications of giving their fingerprints, schools must fully involve parents in order to ensure that the information is obtained fairly. The guidance added that in view of the sensitivity of the issue and the importance of parents' role in education, it would be a heavy-handed approach for schools not to respect the wishes of those pupils and parents who object to school fingerprinting initiatives.[42]

Opponents of using biometric technologies in schools have argued that the practice stigmatises those who have their fingerprints taken and teaches children that giving up important personal information is perfectly routine and mundane. They state that there has been little attempt to inform parents and the general public about the practice. There have been calls for a reassessment of the legislation relating to the use of biometric information in schools.[43] Whether the collection of biometric data in schools is "proportionate" to comply with European legislation has been raised.[44]

The Coalition Programme of May 2010 said that the Government would "outlaw the finger-printing of children at school without parental permission."[45]

In September 2010 the Department for Education carried out "an informal consultation"[46] with interest groups, all of whom, the DFE said, were broadly supportive of the proposed policy.[47] Action on Rights for Children (ARCH) welcomed the requirement for a dual consent of both children and parents before fingerprints could be taken; it wanted the legislation to cover all biometric systems.[48]

The Association of Schools and College Leaders (ASCL) said that the same rules should apply to schools and colleges; however, it expressed concern about placing new bureaucratic burdens on schools and colleges, and wanted an "opt-out" approach rather than 'a need to collect innumerable signatures."[49] The Association of Colleges (AOC) also said that there should be equal treatment for all young people regardless of the institution attended.[50] Liberty welcomed the Government's commitment to require written parental consent before biometric data could be obtained from children; however, it did not believe that it was necessary for schools to obtain such data, and was concerned about the message it gave children about the value of personal privacy.[51]

---

42 ICO, *The use of biometrics in schools*, August 2008

43 "From Finger-painting to Fingerprinting: The Use of Biometric Technology in UK Schools", Emmeline Taylor (Director of Aptus Research and Consultancy), *Education Law Journal*, 2010, pp 276- 288

44 "Europe tells Britain to justify itself over fingerprinting children in schools", *Telegraph*, 14 December 2010; "Collecting children's fingerprints must be validated", *Privacy & Data Protection*, January 2011, p20

45 HM Government, *The Coalition: our programme for government*, May 2010, p11

46 This took the form of a DFE letter to interested groups (source DFE).

47 DFE, *Protection of Freedoms Bill*, *Impact assessment: biometrics in schools and introduction of parental consent*, p15

48 ARCH, *Response to the DFE consultation on fingerprint use in schools*, 21 September 2010

49 ASCL, *Use of biometric recognition systems and students under age 18 in colleges*, 6 October 2010

50 AOC, *Coalition commitment to outlaw the fingerprinting of children at schools without parental consent: A submission from the AOC*, September 2010

51 *Liberty's response to the Home Office's 'Your freedom' consultation*, October 2010, p22 to 24

The DFE's *Business Plan 2011-2015* said that the Department would "no longer continue with programmes that should never have started, because they were the wrong thing to do, such as ContactPoint and the use of fingerprinting in schools."[52]

3.2 The Bill's provisions

Part 1, Chapter 2 of the Bill would require schools and further education institutions to:

- obtain the written consent of parents (or others with main parental responsibility) before processing biometric information from children under the age of 18 years;
- ensure that such information is not processed if a child objects, even where a parent has consented; and
- provide reasonable alternative arrangements for pupils who refuse or whose parents do not consent to biometric information being processed.

Clause 26(1)(2) would require the "relevant authority" for a school, 16 to 19 academy[53], or further education institution to ensure that a child's biometric information must not be processed unless each parent gives their consent subject to certain exceptions as set out in **clause 27** (where the parent cannot be found, where the parent lacks the mental capacity to consent or where the child's welfare requires that the parent is not contacted, for example). A 'child' is defined as a person under the age of 18. A 'relevant authority' means the proprietor of a school or a 16 to 19 academy or the governing body of a further education institution.

Even where parental consent has been given, the processing of such data must not take place if the child objects (**clause 26(4)**). Consent may be withdrawn at any time, and any consent and withdrawal must be made in writing (**clause 27(2)(3)**).

Schools and colleges would be under a duty to provide a reasonable alternative to a biometric system where the child objects to the processing of his or her biometric information, or where any parent does not consent to such processing. Such alternatives must allow the child to access any facility that they would have had access to if using the biometric system (**clause 26(6)**).

Clause 28 defines various terms in relation to clauses 26 and 27 including the meaning of "biometric information," "child", "parent", "parental responsibility", "processing", "proprietor", "relevant authority", "further education institution", and "school". Biometric information is defined as information about a person's physical or behavioural characteristics which can be used to identify that person and is obtained for that purpose. **Clause 28(3)** provides a non-exhaustive list of biometric information that includes data pertaining to fingerprints, skin patterns, features of a person's palm, features of a person's eye, and information about a person's voice or handwriting.

Explaining the rationale for the proposed changes, the Government stressed the importance of protecting the public's fundamental civil liberties and freedoms, and said that the current regulation under the DPA as well as guidance from the ICO and Becta does not appear to have been forceful or clear enough to protect these rights. It is anticipated that the provisions, if enacted, will come into force no sooner than January 2012.[54] The *Explanatory*

---

52 DFE, *Business Plan 2011-2015,* November 2010, p3

53 16 to 19 academies are proposed under the *Education Bill*, Bill 137, currently before Parliament

54 DFE, *Protection of Freedoms Bill*, *Impact assessment: biometrics in schools and introduction of parental consent*, p15

Notes on the Bill estimate the cost of the proposed changes.[55] Human rights issues arising from the provisions are considered in the *Protection of Freedoms Bill European Convention on Human Rights Memorandum by the Home Office.* This notes that the current law relating to parental consent generally is not set out in any clear or coherent legal framework, and that the additional safeguards in the Bill relating to the processing of a child's biometric information would enhance the rights of a child under Article 8 of the ECHR.[56]

4 Regulation of surveillance

Surveillance, in its many forms, is a frequently deployed tool, not least for the purposes of crime prevention and detection.[57] At the same time it intrudes, of necessity, into the private lives of individuals. Existing legislation aims to balance sometimes conflicting factors and, in this context, key legislation is the *Regulation of Investigatory Powers Act 2000* (RIPA). The references it contains to proportionality and necessity are backed up by other legislation such as the *Data Protection Act 1998* and the *Human Rights Act 1998*. The *Protection of Freedoms Bill*, Bill 146 2010-11, focuses on CCTV (which is relatively unregulated) and on the introduction of judicial safeguards for some aspects of surveillance covered by RIPA.

4.1 Regulation of CCTV and other surveillance camera technology

No-one knows how many CCTV cameras are currently deployed and how many are actually functioning. A rough estimate of 4.2 million cameras is often cited, backing up assertions that the UK may already be a "surveillance society".[58] During the House of Commons debate on the relevant part of the Queen's Speech in June 2010, neither the Deputy Prime Minister (Nick Clegg) nor the Home Secretary (Theresa May) elaborated on the Government policy that CCTV should be "properly regulated."[59] The next sections outline the current framework and some commentary on it, before going on to describe and discuss the provisions of the *Protection of Freedoms Bill 2010-11*.

Current framework

CCTV in non-domestic settings is subject to the *Data Protection Act 1998*. The Information Commissioner's Office has issued guidance in the form of a code of practice[60] to help organisations who use CCTV to comply with the Act. An introduction to the guidance comments:

> Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. Most uses of CCTV by organisations or businesses will be covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.

The CCTV code of practice includes specific advice on how CCTV cameras should be deployed and how captured images may be processed (obtained, recorded, held, used, disclosed, erased) in ways that are consistent with the data protection principles that form the backbone to the 1998 Act.[61] These principles require that personal data should be processed fairly and place restrictions on its use, quantity, retention and storage.

---

55 *Explanatory Notes*, paragraph 397

56 *Protection of Freedoms Bill European Convention on Human Rights Memorandum by the Home Office*, paragraphs 45 to 64

57 House of Commons Library Standard Note SN/HA/5624, *CCTV and its effectiveness in tackling crime*, 1 July 2010

58 *A Report on the Surveillance Society*, Surveillance Studies Network, September 2006

59 HC Deb 7 June 2010 cc25-131

60 Information Commissioner's Office, *CCTV code of practice*, Revised edition 2008

61 Section 4(4) and Schedule 1, *Data Protection Act 1998*

On a point unrelated to data protection as such, the CCTV code of practice refers to situations where a licence is required to operate CCTV:

> If the CCTV system covers a public space, the organisation operating the CCTV system should be aware of the possible licensing requirements imposed by the Security Industry Authority.
>
> A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services. Under the provisions of the Private Security Industry Act 2001, it is a criminal offence for staff to be contracted as public space surveillance CCTV operators in England, Wales and Scotland without an SIA licence.

More information on these requirements is available on the website of the Security Industry Authority.[62]

Commentary

In February 2009, the House of Lords Select Committee on the Constitution published a report, *Surveillance: citizens and the state.* The use of CCTV for law enforcement and public safety was among the aspects of surveillance covered, leading to the following recommendation:

> 219. We recommend that the Government should propose a statutory regime for the use of CCTV by both the public and private sectors, introduce codes of practice that are legally binding on all CCTV schemes and establish a system of complaints and remedies. This system should be overseen by the Office of Surveillance Commissioners in conjunction with the Information Commissioner's Office.

While the Labour Government did not accept[63] the Committee's call for a statutory regime for CCTV, it did go on to appoint an interim CCTV regulator[64] whose role was described in a parliamentary written answer in March 2010:

> The Interim CCTV regulator is currently responsible for the development of policy on matters surrounding the use of CCTV in public places. His forward work programme will focus on scoping the need for and requirements of a possible regulatory framework, which could include standards, data retention, training, and a complaints process. He will work with local authorities and other key stakeholders to achieve this.[65]

The Bill's provisions

Chapter 1 of Part 2 of the Bill makes provision for the Secretary of State to prepare a code of practice for surveillance camera systems, including CCTV and Automatic Number Plate Recognition systems. This code will be overseen by a new Surveillance Camera Commissioner.

Clause 29 requires the Secretary of State to prepare a code of practice containing guidance about surveillance camera systems. The clause is fairly flexible as to what such a code should contain and what types of camera surveillance system it should apply to. The code would have to contain guidance about the development *or* use of surveillance cameras

---

62 www.sia.homeoffice.gov.uk

63 House of Lords Constitution Committee, *Analysis of the Government's response to Surveillance: Citizens and the State*, HL Paper 114 2008-09

64 "Interim CCTV regulator is appointed", *public.service.co.uk*, 16 December 2009

65 HC Deb 3 March 2010 c1245W

and/or the processing[66] of images obtained from such systems. Subsection 3 lists in more detail the matters the code could include; these include the justification for deploying surveillance cameras, their location and use, and procedures for complaints or consultation.

In the course or preparing the code, clause 29(5) would require the Secretary of State to consult representatives of persons likely to be under a duty to have regard to it. Among others that would have to be consulted are the Information Commissioner, the Chief Surveillance Commissioner and the new Surveillance Camera Commissioner (which might presuppose the latter to have been appointed ahead of the code's preparation).[67]

Clause 30 sets out the parliamentary procedure for approving the first surveillance camera code of practice. The Secretary of State would have to lay before Parliament the code and a draft order providing for it to come into force. The order would be subject to the affirmative resolution procedure. In the absence of parliamentary approval, the Secretary of State would have to prepare another code of practice under clause 29. Clause 30(7) would prevent the draft order being treated as a hybrid instrument – effectively preventing groups of individuals or bodies especially prejudiced by a surveillance camera code from making formal representations to the Hybrid Instruments Committee.[68] The Bill's explanatory notes do not speculate as to situations where a draft order here could have been ruled to be a hybrid instrument. However, it would seem likely that affected groups would be able to air their views as part of the consultation process attending the preparation of the code of practice.

Clause 31 would require the Secretary of State to keep the surveillance camera code under review and allow her to prepare an alteration to the code or a replacement. Before preparing such an alteration or replacement, the Secretary of State would again have to consult the persons specified in clause 29(5). The Secretary of State would have to lay before Parliament such an alteration or replacement code; this would come into effect if neither House passed a resolution refusing to approve it within 40 days. Subsections 8 and 9 detail how the 40-day period is to be calculated (it excludes periods more than four days when neither House is sitting). If either House disapproved the code, the Secretary of State could still lay a new alteration or replacement, subject to the same procedure.

Clause 32 would require the Secretary of State to publish the surveillance camera code together with any replacement or alteration.

Clause 33 would require a "relevant authority" to have regard to the surveillance camera code in connection with the use, or intended use, of systems covered by the code. Subsection 5 identifies the relevant authorities as being local authorities (England and Wales), police and crime commissioners and chief officers of police. Significantly, in view of the wide range of situations where CCTV cameras are deployed, there is provision for extending the code's provision to other persons.[69] The relevant mechanism would take the form of an order made by statutory instrument and subject to the affirmative resolution procedure. It could not be treated as a hybrid instrument.[70] Before making such an order, the Secretary of State would have to consult a similar range of people as when the original surveillance camera code was being prepared. In particular, this would include people representing the views of those to whom any such order applied. The order could restrict the specification or description of a person to that of the person when acting in a specified capacity or way (subsection 6). The Bill's explanatory notes state that:

---

66 "Processing" is to be given the same meaning as in the *Data Protection Act 1998*
67 Clause 29(5)(c) and clause 35(2)(a)(i)
68 Bill 146 – EN (paragraph 139)
69 Clause 33(5)(k)
70 Clause 33(10)

> This is intended to provide for those instances where certain bodies have dual or multiple roles or, for example, exercise both public functions and private sector functions, and where the duty to have regard to the code may therefore be limited to the exercise of one, or one part of, their functions.[71]

One possible (future) example might be a private investigator engaged by a public authority. In such a capacity, and if a relevant order were to be made and approved by Parliament, the individual would then have to have regard to the surveillance camera code. It may nonetheless be noted that the distinction between public and private sector functions is becoming blurred, at least in the human rights arena, as courts could "horizontally" apply standards intended for public authorities.

A failure to follow the surveillance camera code would not of itself make a person liable to criminal or civil proceedings.[72] However, the code would be admissible in evidence in any such proceedings[73] allowing a court or tribunal to take into account any failure to have regard to the code.[74] The Bill's explanatory notes do not speculate as to situations which might lead to the code coming up in court, but data protection and harassment come to mind.

Clause 34 provides for the appointment by the Secretary of State of a Surveillance Camera Commissioner. The Commissioner would not have enforcement powers (unlike the Information Commissioner for example) but would have the functions of encouraging compliance with the code, reviewing its operation and providing advice. The clause also makes provision for the Surveillance Camera Commissioner to be paid and to be provided with staff, accommodation, equipment and facilities. The total cost has been estimated as £250,000 per annum.[75]

Clause 35 would require the Commissioner to give an annual report to the Secretary of State which the latter would have to lay before Parliament. The Commissioner would also have to publish this report.

4.2 Safeguards for certain surveillance under RIPA

The *Regulation of Investigatory Powers Act 2000* (RIPA) provides a framework for lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources (undercover agents).[76] A recent focus, at least in the context of the recent counter-terrorism review,[77] has been in the use of RIPA powers by local authorities and access to communications data more generally. The *Protection of Freedoms Bill 2010-11* does not concern itself with interception and intrusive surveillance, the latter generally involving interference with private property.

Current framework

RIPA's associated codes of practice lay stress on the need for exercising investigatory powers in ways that are both necessary and proportionate. RIPA itself sets out the possible justifications, such as national security, for interference with an individual's right to privacy embodied by the *Human Rights Act 1998*.

---

71 Bill 146 – EN (paragraph 143)
72 Clause 33(2)
73 Clause 33(3)
74 Clause 33(4)
75 Bill 146 – EN (paragraph 398)
76 In Scotland, surveillance and covert human intelligence sources fall within the *Regulation of Investigatory Powers (Scotland) Act 2000*
77 *Review of counter-terrorism and security powers*, Cm 8004, January 2011

Local authorities can gain access to communications data (often telephone billing information) – but only for the purpose of preventing or detecting crime or of preventing disorder.[78] They can similarly conduct directed or covert (but not intrusive) surveillance operations but may not intercept communications. New (April 2010) codes of practice have been issued in relation to covert surveillance and property interference and to the use of covert human intelligence sources. These new codes formed in part a response to concerns that local authorities were sometimes using their surveillance powers disproportionately.

Part I, Chapter II of RIPA covers the acquisition and disclosure of communications data. Only persons designated under the Act, or by regulations made under it, may authorise access to communications data. And they can only do so for certain purposes (which vary according to the relevant public authority in question).

Orders have subsequently been made by the Secretary of State which have added substantially to the number of public authorities that may access communications data, for specified purposes.[79] Access to communications data requires authorisation of a senior official; the relevant ranks are specified in the *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480.

Surveillance by relevant public authorities, and private companies acting on their behalf, is also subject to the *Regulation of Investigatory Powers Act 2000* (RIPA). A public authority is a relevant public authority if it is specified in Schedule 1 of the RIPA – as amended by secondary legislation.[80]

Of relevance is *Decision No. IPT/03/32/H* (14 November 2006) in the Investigatory Powers Tribunal from which the following is extracted:

> Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not *require* prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful.[81]

Oversight of access to communications data (and interception of its content) is carried out by the Interception of Communications Commissioner. The Office of Surveillance Commissioners is responsible for oversight of property interference under Part III of the *Police Act 1997*, as well as surveillance and the use of covert human intelligence sources by all organisations bound by RIPA (except the Intelligence Services).[82] The Investigatory Powers Tribunal investigates complaints about the use RIPA powers.

Commentary

Among the areas covered by the *Review of counter-terrorism and security powers* (Cm 8004, January 2011) were the following:

---

78 *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480

79 The most recent order, superseding three earlier ones, is the *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480

80 *Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order* SI 2000/2417
Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order SI 2005/1084
Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order SI 2006/1874

81 Investigatory Powers Tribunal Decision No: IPT/03/32/H, 14 November 2006

82 The Investigatory Powers Tribunal website, accessed 22 February 2011

> The use of the Regulation of Investigatory Powers Act 2000 (RIPA) by local authorities and access to communications data more generally

Responding to the review, in a statement to the House of Commons, the Home Secretary said:

> On the Regulation of Investigatory Powers Act 2000, we will implement our commitment to prevent the use of these powers by local authorities unless for the purpose of preventing serious crime and unless authorised by a magistrate. In this context, surveillance-the most controversial power-will be authorised for offences that carry a custodial sentence of at least six months.[83]

The counter-terrorism review recognised the present Government's commitment to introduce tighter regulation on the use of RIPA powers by local authorities. It further acknowledged that local authorities have been criticised for using covert surveillance in less serious investigations including, for example, dog fouling or checking an individual resides in a school catchment area. What is less clear is the scale of the problem. The most recent reports by the Commissioners with oversight of RIPA exhibit relative satisfaction with the operation of the current system.

The *Report of the Interception of Communications Commissioner for 2009* comments:

> 3.43 I am aware that some sections of the media continue to be very critical of local authorities, and there are allegations that they often use the powers which are conferred upon them under RIPA inappropriately. However, I can state that no evidence has emerged from the inspections, which indicates communications data is being used to investigate offences of a trivial nature, such as dog fouling or littering. On the contrary it is evident that good use is being made of communications data to investigate the types of offences which cause harm to the public …

However, there have been reported incidents of surveillance being used for offences of a "trivial nature".[84] Even so, the *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009* states:

> 5.4. I am satisfied that in general the use made of the legislation for which I have the responsibility of oversight is proper and of a good standard. This applies to all types of public authority. Error is usually due to inexperience resulting from lack of use. The lack of use is because most public authorities use the power as the last resort. This is what the law requires.

The Bill's provisions

Chapter 2 of Part 2 of the Bill provides for judicial approval of those types of RIPA surveillance which are available to local authorities. The relevant surveillance activities are access to communications data (**clause 37**) and use of directed surveillance and covert human intelligence sources (**clause 38**). Each of the two clauses in this chapter set out the authorisations that would require judicial approval and the procedure for such approval.

Clause 37 inserts two new sections, 23A and 23B, into RIPA. In general, access to communications data requires authorisation by a "designated person" in the relevant public authority and a notice to be given to a communications service provider. Under new section 23A(2) such an authorisation or notice would require judicial approval before it could take effect. The relevant judicial authority would be a justice of the peace in England and Wales,

---

83 HC Deb 26 January 2011 c307

84 "Councils admit using spying laws", *BBC News*, 23 June 2008

a sheriff in Scotland and a district judge (magistrates' courts) in Northern Ireland. As the Bill stands, the "relevant person" to whom this judicial oversight would apply is restricted to an official of a local authority. However, this could be extended to officials in other public authorities by an order made by the Secretary of State; such an order would be subject to the affirmative resolution procedure.

In determining whether to give approval to the granting or renewal of an authorisation to access communications data, the judicial authority has to be satisfied that there were, and remain, reasonable grounds for believing this to be both necessary and proportionate. These conditions appear, respectively, in sections 22(1) and 22(5) of RIPA. The judicial authority must also be satisfied that "relevant conditions" were satisfied. These conditions relate to the rank of the authorising official and the reasons for the authorisation. In the case of local authorities the official must be a designated person: a Director, Head of Service or Service Manager grade or equivalent. And the only allowable justification in such cases is for the purpose of detecting crime or preventing disorder.[85] New section 23A(5) provides for other conditions to be applied, as specified by an order made by the Secretary of State. This would be relevant, for example, were judicial approval to be extended to public authorities other than local authorities. Orders under new section 23A(5) would be subject to the negative resolution procedure.[86]

Similar criteria apply to judicial approval of a notice to a communications service provider to obtain and disclose data.[87]

New section 23B sets out the procedure for obtaining judicial approval for an authorisation or notice to obtain communications data. In keeping with the covert nature of these investigatory powers there is no requirement to inform the subject of the authorisation or notice. Under subsection 3 the judicial authority may make an order quashing the authorisation or notice under consideration.

Clause 38 makes provision for judicial approval of directed surveillance and covert human intelligence sources. It is broadly analogous to the communications data provisions in clause 37 with the notable exception that it does not extend to Scotland. This is because these two surveillance methods are covered by separate, devolved legislation: the *Regulation of Investigatory Powers (Scotland) Act 2000*. The clause inserts two new sections, 32A and 32B, into RIPA. The former covers authorisations for directed surveillance[88] and covert human intelligence sources[89] under, respectively, sections 28 and 29 of RIPA. New section 32B gives the judicial authorities (magistrates) the power to quash an authorisation for the use of either directed surveillance or of covert human intelligence sources. It also applies conditions to the renewal of authorisations[90] for the conduct or use of covert human intelligence sources: the judicial authority has to be satisfied with the outcome of a review (by the public authority) of the uses made of the covert human intelligence sources. Local authorities use such sources in test purchase operations to investigate under-age sales of products such as alcohol and tobacco.

Judicial authorisation would be needed for either directed surveillance or covert human intelligence sources by dint of new section 32A(2). In both cases the relevant judicial authority would have to be satisfied of there being, and remaining, reasonable grounds for the deployment of these surveillance methods. The reasonable grounds include tests of

---

85 *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480
86 Section 78, RIPA
87 New section 23A(4)
88 New section 32A(3),(4)
89 New section 32A(5),(6)
90 Renewals are treated in the same way as grants by dint of section 43(5) of RIPA.

necessity and proportionality and, in the case of covert human intelligence sources, reasonable belief that specified[91] supervision arrangements are in place. At the time of the public authority granting an authorisation there is also a requirement for "relevant conditions" to be in place. As with access to communications data, these relate to the rank of the official granting the authorisation and the reasons for it being granted. The reasons, linked to the necessity test, are restricted, in the case of local authorities, to the purpose of preventing or detecting crime or of preventing disorder.[92] The Bill's explanatory notes (paragraph 30) signal that a seriousness threshold for crime will be introduced through an order made under section 30(3)(b) of RIPA. There is scope for imposing any other relevant conditions on local authorities by an order,[93] subject to negative resolution,[94] made by the Secretary of State.

Clause 38 also includes provision for imposing[95] (by negative resolution order)[96] any relevant conditions on persons who might subsequently become relevant for the purposes of judicial approval. Adding persons from public authorities other than local authorities would require an order to be made by the Secretary of State,[97] subject to affirmative resolution.[98]

Examples of the powers

The police have powers to enter and search buildings under many Acts. Some of these powers are general ones, and some are specific ones to deal with particular crimes, such as drug offences or possession of offences weapons.

Fire officers have powers to enter buildings in emergencies. There are powers to deal with the safety of public utilities. Under the *Gas Act 1986*, for example, an authorized officer can enter a consumer's premises to inspect gas fittings.

There are many powers of entry for local authority officers, for example to enforce environmental health law, or to check for breaches of planning controls.

Customs and Excise officers have some very wide powers to enter premises, in some cases without warrants or reasonable suspicion.

Other powers affect specific industries such as agriculture and fishing.

5 Powers of entry

5.1 Background

Chapter 1 of Part 3 of the Bill is concerned with rationalising the vast array of powers various kinds of officials have to enter people's homes and businesses without their permission.

The courts have long recognised that "a man's home is his castle",[99] and that state officials should not be able to enter property without the owner's consent unless there is an explicit power to do so. If an official enters a property without permission and without a legal power, then this could be a trespass, and he or she could be sued.[100] Therefore, as the scope of the state has expanded since the middle of the 20th century, Parliament has granted a very large number of specific powers of entry for officials from central and local government, inspectorates and other bodies. Around 250 of these powers derive

91 Sections 29(2), 29(7)(b), RIPA

92 *Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order* SI 2010/521

93 New sections 32A(4)(a)(iii), 32A(4)(b)(iii) for directed surveillance and new sections 32A(6)(a)(iii). 32A(6)(b)(iii) for covert human intelligence sources.

94 Section 78, RIPA

95 New section 32A(4)(c) for directed surveillance and new section 32A(6)(c) for covert human intelligence sources.

96 Section 78, RIPA

97 New section 32A(7)

98 New section 32A(8)(a)

99 Sir Edward Coke, *The Third Part of the Institutes of the Laws of England, or, A Commentary on Littleton,* 1669 edition, p161

100 There are exceptions when consent can be implied by necessity, for example in emergencies

from regulations made under the *European Communities Act 1972*.[101]

Warrants and the use of force

"Force" can include the application of any physical force to any part of a structure to gain access without the permission of the owner; so it could be as little as moving a door which is already ajar.[102] Some of the statutory powers specifically allow for the use of force where necessary, whilst others are silent on this. However, where there is no explicit authorisation of force, the courts have accepted that this may still be used sometimes if permission is refused.

Some entry powers require a warrant to be obtained; some do not. Some permit entry without warrant, but allow for a warrant to be obtained.

A 2007 study by the Centre for Policy Studies[103] identified four categories:

- where force can be used immediately
- where a warrant must be obtained before entering
- where entry can be effected without a warrant, but a warrant could still be obtained
- where there is no mention of force and no warrant available

The study noted, in relation to the third category:

> Because of the option to obtain a warrant, courts have usually interpreted such powers as providing that any entry without a warrant must not involve the use of force.

Many of the powers have penalties for obstructing the person with a right of entry. These vary considerably; some involve fines, and others imprisonment. So if a person refuses entry under a power which does not include the use of force, he may still face sanctions.

Human rights

The *Human Rights Act 1998* means that public authorities must act in accordance with Article 8 of the European Convention on Human Rights, which provides for the right to respect for family life and the home.[104]

How many powers of entry are there?

Until very recently, nobody knew how many statutory powers of entry there were. Over time, many government departments have sponsored reams of primary and secondary legislation conferring these powers on officials, so collecting them all together represented a major task. Legal textbooks[105] set out a large number of them, but there was no official, central list.

---

101 Source: Home Office, *Primary Legislation: Powers of Entry* and *Secondary Legislation: Powers of Entry*, 11 February 2011, available from the *Powers of Entry* page on the Home Office Website [on 18 February 2011]

102 *Swales v Cox* [1981] QB 849

103 Harry Snook, *Crossing the Threshold: 266 ways the State can Enter your Home*, Centre for Policy Studies, 2007, ch7

104 See p7 of this Research Paper above.

105 Notably Richard Stone's, *The Law of Entry, Search and Seizure*, 2005

A Home Office Analysis of existing provisions,[106] which began under the previous government in 2007, has identified a total of **1227 statutory powers of entry** as of November 2010:

- 749 in primary legislation
- 478 in secondary legislation.

5.2 Pressure for change

These individual powers of entry were obviously seen by governments of the day as sensible and necessary when they were introduced. However, those who have campaigned on this issue argue that the combined effect makes it impossible for ordinary people to be aware of their rights. The Centre for Policy Studies report states:

> As a result of the proliferation and variety of entry powers, a citizen cannot realistically be aware of the circumstances in which his home may be entered by state officials without his consent, or what rights he has in such circumstances.[107]

There have been concerns about this proliferation of powers for many years. In the late 1970s, a campaign by the National Association of Self Employed led to a Government review of statutory powers to enter business premises.[108]

The Conservative peer Lord Selsdon has been working on this issue since the 1970s. Between 2006 and 2010, he introduced five Private Member's Bills.[109] Two of these completed their passages through the Lords, although they made no progress in the Commons.[110] The broad aims of the bills was to ensure that an official, whether of government or of another organisation, would not be able to enter somebody's property and seize or search without permission or without a court order.

The 2007 report by the Centre for Policy Studies also concluded that legislation was needed to reform these powers:

- Entry powers are in serious need of reform. A new Act of Parliament should harmonise the procedural provisions of all existing entry powers and protect the citizen by making accountability and transparency paramount.
- Officials should always seek permission to enter a home if possible, even when they have a power to enter without it.
- A reasonable time for entry should be specified.
- With the exception of the emergency services, state officials should always have to get a warrant from a magistrate before they can force entry to a private home. The magistrate should carefully scrutinise their case and refuse a warrant where it is unnecessary.

---

106 Home Office, *Primary Legislation: Powers of Entry* and *Secondary Legislation: Powers of Entry*, 11 February 2011, available from the *Powers of Entry* page on the Home Office Website [on 18 February 2011].

107 Harry Snook, *Crossing the Threshold: 266 ways the State can Enter your Home*, Centre for Policy Studies, 2007, summary, p(i)

108 HC Deb 06 December 1979 vol 975 cc277-8W

109 Each was called *The Powers of Entry (etc.) Bill*: See HL Bill 57 of 2005-06; HL Bill 5 of 2007-08; HL Bill 71 of 2007-08; HL Bill 12 of 2009-10; and HL Bill 42 of 2009-10

110 For the debates on these, see *Bill stages — Powers of Entry etc. Bill [HL] 2009-10* and *Bill stages — Powers of Entry etc. Bill [HL] 2007-08*, on the Parliament website [on 18 February 2011]

- The exercise of entry powers should be thoroughly documented, and statistics on their use made public. This will put pressure on officials to use them in a reasonable and proportionate manner. [111]

The Home Office Review

In the Second Reading debate of his most recent Bill, Lord Selsdon described how he and his colleagues had taken the matter up in October 2007 with then Prime Minister, Gordon Brown:

> When I introduced the last Bill, I went to see the noble Lord, Lord West, who was very helpful but did not really want to do anything - or his further authorities did not want to do anything. So we thought that we should quietly let No. 10 know that there was a Bill. A few days later, on 25 October, the Prime Minister got up and made a "liberty" speech, as it was called, about the freedom of the individual and the need to deal with these powers of entry. That started the movement.[112]

In the speech Lord Selsdon mentioned, Gordon Brown promised a review:

> There are a surprisingly high number - at least 250 - of provisions granting power to enter homes and premises without permission.
>
> This high number reflects how often they are drawn very narrowly - not least because of our traditional respect for liberty and privacy.
>
> I share the concerns about the need for additional protections for the liberties and rights of the citizen.
>
> And I believe that one of the strongest guarantees is a clear understanding of what these rights are and that is more difficult with the very existence of hundreds of laws.
>
> (...)
>
> So, alongside the review of police powers, the Home Secretary will establish and coordinate a wider review of all other powers of entry.[113]

Details of the Home Office review are available on the archived Home Office website.[114]

Conservative and Liberal Democrat policy

The 2010 Conservative Manifesto promised:

> We will take further steps to protect people from unwarranted intrusion by the state, including:
>
> - cutting back intrusive powers of entry into homes, which have been massively extended under Labour[115]

The Liberal Democrat manifesto did not specifically mention these powers, and neither did the Coalition Programme.

---

111 Harry Snook, *Crossing the Threshold: 266 ways the State can Enter your Home*, Centre for Policy Studies, 2007, summary p (ii)
112 HL Deb15 January 2010 c719
113 " In full: Brown speech on liberty", *BBC News*, 25 October 2007
114 Home Office website on The National Archives, *Operational Policing: Review of Powers of Entry* [on 18 February 2011]
115 p79

5.3 The Bill's provisions

Schedule 2 repeals some specific powers of entry, and **clause 39** would enable ministers (including Welsh Ministers) to repeal further "unnecessary or inappropriate" powers by order. **Clause 40** would allow ministers to add safeguards to existing powers by order, and **clause 41** would allow them to rewrite them by order. Under **clause 43**, they would have to consult before modifying powers under clauses 39 to 41.

Clause 42 would give each Secretary of State a duty to review certain existing powers of entry, and to report to Parliament.

Clause 47 would require the H to prepare a code of practice with guidance on the exercise of powers of entry.

6 Wheel clamping and parking on private land

Clauses 54 to 56 and **Schedule 4** to the Bill provide for the prohibition of wheel clamping of vehicles parked on private land and provide for alternative remedies for landowners.

6.1 Ban on wheel clamping

Background

Wheel clamping on private land has been a major problem for some years. The legality of wheel clamping on *public* land is clearly set out in legislation but on *private* land, including car parks, it has not expressly been provided for in law.[116] As a result there has been considerable controversy about the behaviour of some private wheel clamping companies and even about the legality of clamping vehicles on private land. The view of successive governments has been that owners of land must be able to take action against those who park without permission and that wheel clamping may be an effective way of dealing with such situations, but that any action must be carried out in a reasonable manner.[117] Cases against wheel clampers are heard in the civil courts.

Clamping companies currently have to be licensed by the Security Industry Authority (SIA).[118] The SIA was set up by the Labour Government in 2005 and the enabling legislation makes it an offence to undertake clamping activities without a licence. However, many of the complaints about wheel clamping operations are about the level of charges, which are not regulated by the SIA. There is a Code of Practice for the industry, published by the British Parking Association (BPA), which sets out recommended charges (fees) for wheel clamping activity and guidance on signage. *However, these charges are only recommendations and have no legal force.* The Labour Government made provision to change that in 2010 and to introduce an independent appeals procedure but the legislation was not brought into force before the 2010 General Election was called.[119]

The Coalition Programme of May 2010 stated that one of the Government's transport priorities was to "tackle rogue private sector wheel clampers".[120] However, it was initially not clear whether they intended to bring the relevant provisions of the *Crime and Security Act 2010* into force or tackle the problem in some other way.[121]

---

116 Background to and full details on the regulation and licensing of wheel clamping on private land are given in Library Standard Note SN/BT/1490, *Parking: wheel clamping*

117 HL Deb 18 December 2000 c577

118 The SIA was set up under the *Private Security Industry Act 2001*

119 See sections 42-44 and Schedule 1 of the *Crime and Security Act 2010*

120 HM Government, *The Coalition: our programme for Government*, May 2010, p31

121 See, for example, HC Deb 15 June 2010 c852

On 17 August 2010 the Home Office Minister, Lynne Featherstone, announced the Government's intention to introduce measures in a "Freedom Bill" to provide for an outright ban of clamping on private land, where it is carried out by private companies. It was envisioned that, when the ban comes into force, the licensing regime provided for in the 2010 Act and outlined above, would be abolished as it would be unnecessary. The provisions of the 2010 Act introduced by the previous Government would therefore not be brought into force.[122]

The Bill's provisions

Clause 54 of the Bill will effectively make it a criminal offence to clamp (immobilise) a vehicle on private land except where one has the lawful authority to do so (for example, on behalf of a local authority, the DVLA or the police). The Explanatory Notes to the Bill have a good explanation of how this will work in practice.[123]

The maximum penalty will be a fine of £5,000 on summary conviction or an unlimited fine on indictment.

Schedule 7, Part 3 abolishes the licensing regime set up under the previous Government and the uncommenced provisions of the 2010 Act (see above).

6.2 Parking on private land

Background

Very generally, what you can do on any private land depends on the extent of your right to be there. Normally the owner of the land gives you permission to be there for certain purposes (for example, in order to use a shop or a surgery); you then agree to come on the land only for those purposes and subject to any other conditions that you may have agreed.

With regard to the imposition and collection of fines, one would expect that signs would be displayed alerting the motorist to the potential consequences of his/her actions when parking the vehicle. It should be clear that parking is not allowed or restricted and that enforcement action will be taken in respect of any subsequent contravention.[124] Any fines levied should also be reasonably proportionate and demanding money with menaces is an offence.

If one chooses not to pay the fine, the company will pursue the ticket through the courts as civil debt. One should seek legal advice when deciding whether or not to pay such a fine.[125]

The British Parking Association has published a Code of Conduct for companies operating parking enforcement on private land but this is not statutory, it is only guidance.[126] The rules for the release of data to private enforcement companies were tightened up from 1 October 2007 to limit the release of vehicle owner information by the DVLA to members of an Accredited Trade Association (ATA).[127] However, this only covered electronic requests for information. In August 2009 the Labour Government announced that the requirement to be a member of an ATA would be extended to companies making manual, paper-based requests.[128]

---

122 Home Office news release, *Government announces ban on wheel clamping*, 17 August 2010
123 Protection of Freedoms Bill - Explanatory Notes, paras 197-200
124 See, for example, HC Deb 10 February 2005 c1706W
125 Information on sources of legal assistance can be found in Library standard note SN/HA/3207
126 BPA press release, *BPA initiative to end rogue ticketing*, 18 April 2007; see also the full Code available on the BPA website
127 DVLA press release, *New Code of Practice issued by Accredited Trade Associations*, 1 October 2007
128 DfT news release, *Government crack down on cowboy parking companies*, 27 August 2009

The Bill's provisions

The Government had not previously indicated that there would be any parking-related measures in the Bill, or in fact that it was planning to make any changes to parking regulation at all. However, once the Government announced its intention to outlaw wheel clamping on private land, concerns were raised that there would be no reliable way for private landholders to remove people parking on their land. The Bill provides two remedies:

Clause 55 amends section 99 of the *Road Traffic Regulation Act 1984* and will permit the Secretary of State to make regulations extending the powers of police and local authorities to remove and dispose of vehicles left "illegally, obstructively or dangerously parked" on any land.

Clause 56 and **Schedule 4** would enable private landowners to recover parking charges from the keepers of vehicles parked on their land where they have in effect entered a contract regarding the conditions upon which they have come onto that land to park. What this means is that where one owns a car park on private land, maintained by a member of an Accredited Trade Association, and abiding by the requirements of that Association (that is, erecting the proper signs, applying maximum charging rules, having a proper complaints and appeals procedure), they will have the ability to recover parking charges from the owner ("keeper") of the vehicle, if the driver does not pay.

Where this marks a change from current practice is that at the moment a landowner only has recourse to the courts if they make a charge for parking on their land but do not enforce it with clamping. The changes outlined in the Bill would allow landowners to recover parking charges without recourse to the courts, a process which can be time consuming and costly. A full explanation of how this new scheme would work is set out in the Explanatory Notes to the Bill.[129]

7 Counter-Terrorism Powers

7.1 Background

Part 4 of the Bill makes changes to certain counter-terrorism powers introduced by the *Terrorism Act 2000* (as amended). These changes were heralded by the publication of the above-mentioned *Review of Counter-Terrorism Powers* in January 2011.

The review focused on six separate areas of policy.[130] This part of the Bill addresses two of those areas, namely the pre-change detention of terrorist suspects and specific stop and search powers. Separate legislation, expected to bring an end to the use of control orders, is due to be published shortly.[131]

7.2 Pre-charge detention

Detailed information about the pre-charge detention regime imposed under the *Terrorism Act 2000*, as amended, can be found in the Library Standard Note SN/HA/5634, *Pre-charge Detention in Terrorism Cases*.

In brief, however, extended pre-charge detention of terrorism suspects was introduced in permanent legislation by section 41 and Schedule 8 of the *Terrorism Act 2000*. The period of detention was increased from 7 days to 14 days under the *Criminal Justice Act 2003*. It was further extended, to a period of 28 days, under the *Terrorism Act 2006*. This in itself was a

---

[129] Protection of Freedoms Bill - Explanatory Notes, paras 204-210

[130] For further information, see: Library Standard Note SN/HA/5852,*The Counter-Terrorism Review*

[131] The Security Minister, Baroness Neville Jones has informed the Home Affairs Select Committee that legislation should be published "before Easter". See: HC 675-iii, 1 February 2011, q 205

compromise, as the Government had originally sought to introduce a 90 day pre-charge detention limit. The 2006 Act introduced a procedural safeguard, so that the maximum period of pre-charge detention would revert to 14 days (the limit established by the *Criminal Justice Act 2003*), after one year, unless renewed by an affirmative order.

Successive twelve month orders were made in 2007, 2008 and 2009 and the previous Government also attempted to extend the maximum period of pre-charge detention to 42 days by way of the *Counter-Terrorism Bill*, which was introduced in the 2007-8 session. The relevant provisions were rejected by the House of Lords. Both the Conservatives and the Liberal Democrats opposed the previous Labour Government's efforts to further extend pre-charge detention. Former Shadow Home Secretary, David Davis, went as far standing down from his front bench post and contesting a by-election on the issue.

Statistics on pre-charge detention

The 14 day detention period came into effect on 20 January 2004 and the maximum period of detention pre-charge was extended to 28 days with effect from 25 July 2006. Table 1 provides details of the numbers of individuals charged or released and held from between 14 to 15 days and through to 27 to 28 days. Use of extended pre-charge detention has declined in recent years. No individual was held beyond 14 days pre-charge detention in 2008/09 or 2009/10 (and only one in 2007/08, who was charged after 19 days).

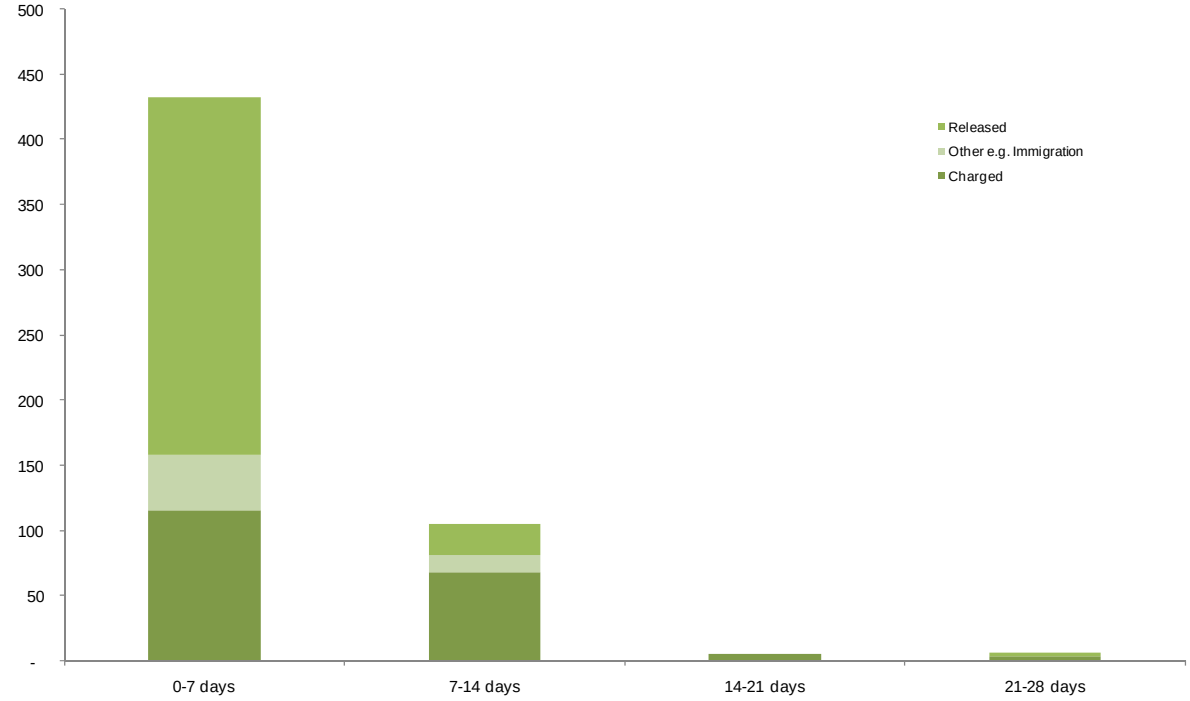
Table 1
Number of individuals held for over 14 days pre-charge detention

Period of detention	Year of arrest	Number of persons held	Charged	Released without charge
14-15 days	2006/07	1	1	
18-19 days	2007/08	1	1	
19-20 days	2006/07	3	3	
27-28 days	2006/07	6	3	3

Source: Table 1.3, Home Office Statistical Bulletin 10/10

Most of those arrested under terrorism powers continue to spend a short time in custody. Between 2006/07 and 2009/10 58% of those released without charge were released within one day and 91% within a week:

Chart 1: Time in days from arrest under s41 of the Terrorism Act 2000 to charge, release without charge or other action taken, 2006/07 - 2009/10



Conservative and Liberal Democrat Policy on pre-charge detention

In June 2008, then Shadow Home Secretary, Dominic Grieve QC, indicated that, if elected, the Conservative party would review the 28 day detention period, which he described as "much longer" than it should be.[132] Following the formation of the Coalition Government, it was hinted that the Government might be willing to scale back the pre-charge detention period.[133] The Liberal Democrat 2010 election manifesto committed to "reduce the maximum period of pre-charge detention to 14 days."[134]

Before the Home Secretary announced the Counter-Terrorism Review, she indicated, in a Written Ministerial Statement of 24 June 2010, that although she wished to renew the 28 day pre-charge detention period for 6 months both parties in the coalition were "clear that the 28-day maximum period should be a temporary measure" and one that the Government would "be looking to reduce over time."[135]

The Counter-Terrorism Review, which was announced in July 2010, had been expected to conclude in November; however the final report was delayed. In answer to an urgent question on 20 January 2011, the Home Office Minister, Damien Green (pre-empting the publication of the review) confirmed that that the Government would not be seeking to extend the order allowing the maximum 28-day limit, and accordingly the maximum limit of pre-charge detention reverted to 14 days as of 25 January 2011.

This process was criticised by the Opposition. In an article in the *Evening Standard*, Shadow Home Secretary Yvette Cooper argued that the Government had taken a "chaotic" approach to national security by allowing the powers to lapse without having been entirely clear what

---

132 "Tories consider terror arrest limit below 28-days", *Daily Telegraph*,14 June 2008
133 "Warsi ready to scrap Tories' A list of women and black candidates", *The Sunday Times,* 13 June 2010
134 *Liberal Democrat Manifesto 2010*, p 95
135 Written Ministerial Statement, HC Deb 24 June 2010 cc20-21WS

emergency powers could be introduced to reinstate extended pre-charge detention if this became necessary.[136]

At present, an order making power (contained in s 25(2) of the 2006 Act) could be exercised at any time to restore extended 28 day pre-charge detention - if the Government laid a draft of the order before Parliament (and it was approved by a resolution of each House). The Government has indicated that should an emergency situation arise, it would like to replace this procedure with emergency powers contained in primary legislation.

Counter-Terrorism Review Recommendations

The Counter-Terrorism Review concluded that the limit on pre-charge detention for terrorist suspects should be set at 14 days, and that limit should be reflected on the face of primary legislation. It made the following recommendations:

> 26. The review concluded that the limit on pre-charge detention for terrorist suspects should be set at 14 days, and that limit should be reflected on the face of primary legislation. The review accepted that there may be rare cases where a longer period of detention may be required and those cases may have significant repercussions for national security.
>
> 27. The review found that there were challenges with many of the options for a contingency power, particularly if it was intended to extend the period of detention during an investigation. Parliamentary scrutiny of a decision to increase the maximum period of detention in the wake of a particular investigation carried some risks of prejudicing future trials and would need to be handled particularly carefully.
>
> 28. The review, therefore, recommends that:
>
> i. The 28 day order should be allowed to lapse so that the maximum period of pre-charge detention reverts to 14 days. The relevant order making provisions in the Terrorism Act 2006 should be repealed.
>
> 29. In order to mitigate any increased risk by going down to 14 days, the review recommends:
>
> ii. Emergency legislation extending the period of pre-charge detention to 28 days should be drafted and discussed with the Opposition, but not introduced, in order to deal with urgent situations when more than 14 days is considered necessary, for example in response to multiple co-ordinated attacks and/or during multiple large and simultaneous investigations.

Lord Macdonald of River Glaven QC, the former Director of Public Prosecutions, who provided independent oversight of the review, produced a report to coincide with the publication of the Counter-Terrorism Review. On the issue of pre-charge detention, he concluded that:

> It is my clear conclusion that the evidence gathered by the Review failed to support a case for 28 day pre-charge detention. No period in excess of 14 days has been sought by police or prosecutors since 2007, and no period in excess of 21 days has been sought since 2006.
>
> Bearing in mind that the power to detain suspects beyond 14 days was always regarded by Parliament as a temporary and quite exceptional measure, this paucity of use in recent years hardly speaks of pressing need.

---

136 "Theresa May must put public safety before politics", *Evening Standard*, 25 January 2011

> Furthermore, on the occasions when the power has been used, it has not always demonstrated its fundamental utility. For example, of the two men charged after 21 days in Operation Overt (the airline plot), one case was stopped by the trial judge, and the second resulted in a jury acquittal.
>
> In the circumstances, the Review is plainly right to recommend that the maximum period of pre-charge detention should be reduced to 14 days.
>
> [...]
>
> I agree with the Review's conclusion that the risk of an exceptional event, requiring a temporary return to 28 days, is best catered for by having emergency legislation ready for placing before Parliament in that eventuality. This is the option most strongly supported by the evidence gathered by the Review.[137]

The draft legislation mentioned in the review was published on 11 February 2011 as the *Draft Detention of Terrorist Suspects (Temporary Extension) Bills*.

The Explanatory Notes to the Draft Bills indicate that both would have the effect of extending the maximum period of pre-charge detention to 28 days for a period of three months[138], should either of them be introduced and approved by Parliament. "One bill could be used immediately while the order-making provisions of the 2006 Act are still in force and the other once those provisions have been repealed."

The draft legislation will be subject to pre-legislative scrutiny. The Government has indicated that it would only be brought forward in "exceptional circumstances."

Terrorism Bail

The review rejected the introduction of a pre-charge conditional bail. This is currently not available for people detained under Schedule 8 to the *Terrorism Act 2000.* The Parliamentary Joint Committee on Human Rights had recommended the introduction some form of bail, but the review concluded that:

> [T]here would be risks for public safety in releasing terrorist suspects when the nature and extent of their involvement in terrorism was still being investigated. Police bail was unlikely, therefore, to be a substitute for extended pre charge detention.[139]

Lord Macdonald took a different approach to terrorism bail, considering it an unnecessary restriction. He said:

> The Review is also right to reject the option of a further 14 days of strict bail being made available to the police. This new restriction would not have been justified by any evidence gathered by the Review, and it would have been widely regarded as an unwarranted form of control order. It is unnecessary.[140]

A permanent reduction to 14 days pre-charge detention

Clause 57 of the Bill would ensure a permanent reduction of the maximum period of pre-charge detention to 14 days. In particular, it would change the wording of Schedule 8 of the *Terrorism Act 2000* and would also omit section 25 of the *Terrorism Act 2006*. This would have the effect of removing the order making power contained in the 2006 Act (ensuring that

---

137 Lord Macdonald QC, Review of Counter-Terrorism Powers (Cm 8003), p 4

138 NB The *Explanatory Notes* to the *Protection of Freedoms Bill* erroneously states that the provisions would last for a period of 6 months

139 Home Office, *Review of Counter-Terrorism Powers*, Cm 8004, 26 January 2011, p11

140 Lord Macdonald QC, *Review of Counter-Terrorism Powers*, Cm 8003, 26 January 2011, p4

it was not possible to reinstate 28 day pre-charge detention through the use of that provision).

7.3 Stops and Searches under the *Terrorism Act 2000*

The police have a number of stop and search powers, the most commonly-used being section 1 of the *Police and Criminal Evidence Act 1984* (PACE). Most of these powers require the police to have some kind of "reasonable suspicion". There are two stop and search powers under the *Terrorism Act 2000*. Section 43 allows the police to search a person for evidence that he or she is a terrorist, but only where they have "reasonable suspicion". The controversial power is under sections 44 to 47 (usually referred to as the "section 44" power). This allows the police to search people and vehicles *without* reasonable suspicion.

However before this power can be exercised, a senior police officer has to have authorised it for an area. This can be done if that senior officer "considers it expedient for the prevention of acts of terrorism." The authorisation for section 44 searches can be for a small area or for the whole police force area. It can last for up to 28 days, although it will cease to have effect unless the Secretary of State confirms it within 48 hours. In London, the provisions have been used to provide rolling authorisations over the whole of the Metropolitan Police force area.

These section 44 powers replaced similar ones which had been brought in by the *Criminal Justice and Public Order Act 1994*.[141] These had been introduced in response to concerns that the police outside Northern Ireland did not have sufficient powers to deal with vehicle bombs and small devices carried by individual terrorists.[142]

The Government acknowledges that the breadth of the section 44 power has meant that the police have found it useful in a range of counter-terrorism operations and situations.[143] However, this breadth has led to concerns about misuse.

How much has the power been used?

Since their introduction, the number of section 44 searches increased considerably in response to the terrorist threat, particularly in London. The predecessor power was used around 1,900 times in 1999-2000; section 44 searches peaked at around 210,000 in 2008/09.. Between 2006/07 and 2007/08 the number of these stops and searches in England and Wales almost tripled. This increase was driven by the Metropolitan Police increase of 266% compared to a more modest 38% increase across all other forces. Table 2 shows the number section 44 searches from 1999/00 to 2008/09 together with the number of resultant arrests.

---

[141] These inserted new sections 13A and 13B into the *Prevention of Terrorism (Temporary Provisions) Act 1989*

[142] The then Home Secretary, Michael Howard, in the Bill's Second Reading debate: HC Deb 11 January 1994 c30

[143] HM Government, *Review of Counter-Terrorism Powers*, Cm 8004, January 2011, p15

Table 2
Stop and Search of pedestrians, vehicles and occupants under sections 44(1) and 44(2) of the Terrorism Act 2000[1] and resultant arrests, England and Wales

		Arrests		
	Total searches [2]	Total	for terrorism offences	for other reasons
1999/00	1,900	18	1	17
2000/01	6,400	45	1	44
2001/02	10,200	489	20	169
2002/03	32,100	380	19	361
2003/04	33,800	491	19	472
2004/05	37,000	468	64	404
2005/06	50,000	563	105	458
2006/07	42,800	495	28	467
2007/08	126,500	1,234	19	1,215
2008/09	210,000	1,245	9	1,236

Notes:

1 Formerly sections 13A and 13B of the Prevention of Terrorism (Temporary Provisions) Act 1989 and repealed under the Terrorism Act 2000 (which came into force on 19 February 2001).

2 Total search figures have been rounded to nearest 100

Source: Table 2c, Police Powers and Procedures, England and Wales 2008/09, Home Office Statistical Bulletin 06/10

Provisional data suggests that there has been a reduction in the use of these powers in 2009/10. The number of searches in 2009/10, excluding vehicle only searches, was 57% lower than the previous year.[144] This fall may in part result from guidance published in 2008 by the National Policing Improvement Agency. This emphasised that the powers were exceptional, that the geographical extent must be clearly defined and that police forces should provide the Home Secretary with a detailed justification and community impact assessments.[145] Final data for 2009/10 will be published in April 2011.

7.4 Objections to the powers

Section 44 is potentially an intrusive power. It allows police to stop people without reasonable suspicion, and to perform a search which can involve the removal of headgear, footwear, an outer coat, a jacket or gloves in public. Failing to stop, or obstructing the police, can result in a six months imprisonment and a £5,000 fine. A number of the concerns raised are discussed briefly below.

Alleged overuse by some forces

The Government's former independent reviewer of terrorism legislation, Lord Carlile of Berriew, repeatedly drew attention in his annual reviews to different levels of use of the power in forces with very similar risk profiles. His 2009 report stated that, whilst he was not in favour of repeal, he was sure the power could safely be used far less:

> It should not be taken that the lesser usage of *section 44* in places other than London means that such places are less safe, or more prone to terrorism. There are different

144 *Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes and stops & searches, Great Britain 2009/10*, Home Office Statistical Bulletin 18/10

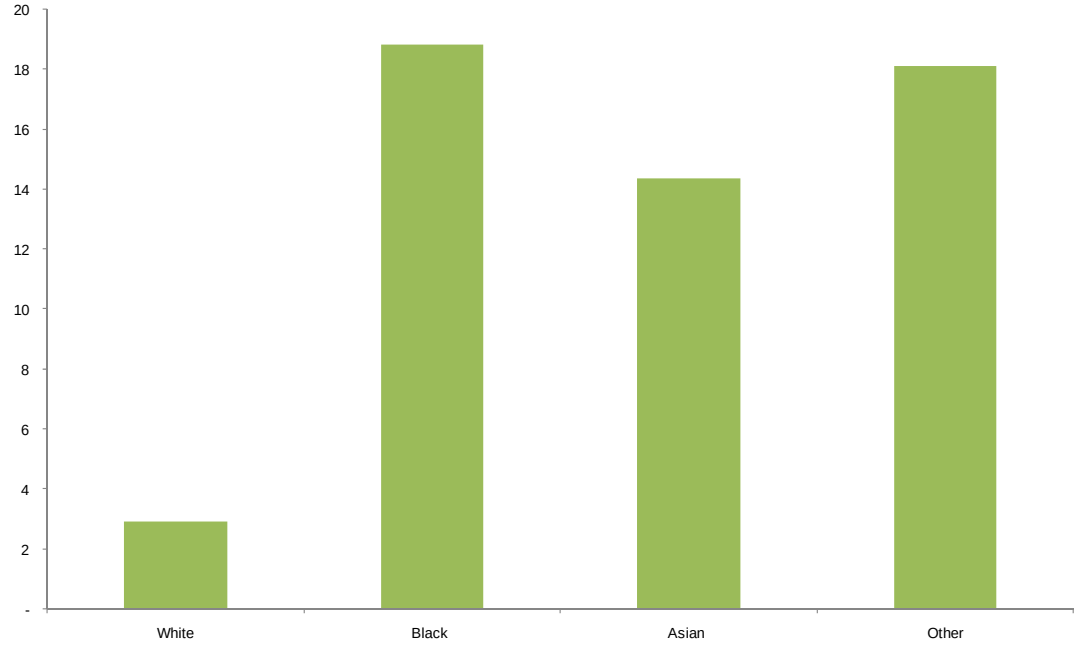
145 National Policing Improvement Agency, *Stop and Search in Relation to Terrorism*, 2008

ways of achieving the same end. The effect on community relations of the extensive use of the section is undoubtedly negative. Search on reasonable and stated suspicion, though not in itself a high test, is more understandable and reassuring to the public.[146]

Disproportionate impact on minorities

Chart 2 shows that in 2008/09 black people were six and a half times more likely to be stopped and Asians five times more likely to be stopped under these powers than their white counterparts:

Chart 2 : Stop and Search of persons under section 44 of the Terrorism Act 2000, per 1,000 population, by ethnicity 2008/09



The publication in April 2009 of Ministry of Justice statistics showing a surge in section 44 stops with the largest increases being for Black and Asian people.[147] This led some commentators to argue that this demonstrated that the powers were being abused.[148] The Ministry said the rise was "directly attributable to the robust response by the Metropolitan police to the threat of terror related networks in London since the Haymarket bomb in 2007."[149]

Damage to community relations

There have been longstanding concerns, not least because of this disproportionality, that the use of section 44 might damage relations with the Muslim community. The Home Affairs Committee examined the issue in its 2005 report, *Terrorism and community relations*.[150]. The Committee did not feel that the Muslim community was being unreasonably targeted, but they acknowledged that the perception of unfair treatment was harmful.[151]

---

146 Lord Carlile, *Report on the Operation in 2008 of the Terrorism Act 2000* and of part 1 of the Terrorism Act 2006, June 2009, p31

147 Ministry of Justice, *Race in the Criminal Justice System* 2007-08, 30 April 2009

148 "Use of stop and search under terror law surges", *Guardian*, 1 May 2009

149 Ministry of Justice, *Race in the Criminal Justice System* 2007-08, 30 April 2009, p30

150 6 April 2005, HC 165 2004-05

151 Paragraph 153

Searches on photographers

The Government's review of terrorism noted that there had been "widespread concern, notably amongst photographers and journalists that counter-terrorism powers, including section 44, were being used to stop people legitimately taking photographs."[152] There have been many complaints from professional and amateur photographers who have been stopped; there have also been concerns about the use of this and other counter-terror powers to prevent the public photographing police officers, for example during demonstrations.

Searches on children

This issue came to the fore in the summer of 2009, when the *Sunday Telegraph* ran a story following responses to Freedom of Information requests by 16 police forces. This reportedly showed that more than 4,000 under 10s had been stopped per year.[153]

7.5 Gillan and Quinton v UK

On 12 January 2010, the European Court of Human Rights (ECtHR) decided, in the case of Gillan and Quinton, that the section 44 provisions violated article 8 of the European Convention on Human Rights.[154] On 30 June 2010, it ruled that the UK could not appeal against the Judgement.

Gillan and Quinton v UK

Kevin Gillan and Pennie Quinton were stopped and searched under section 44 on their way to an arms fair in September 2003. They challenged the exercise of these powers on the grounds (amongst others) that this had constituted an interference with their right to respect for private and family life under Article 8 of the European Convention on Human Rights. They lost their judicial review case in October 2003, and their appeal in July 2004. The House of Lords also found against them on 8 March 2006.

However, on 12 January 2010, the European Court of Human Rights (ECtHR) found against the UK Government. Of particular concern was the fact that the powers could be triggered on the ground of "expediency" in the fight against terrorism, which the ECtHR felt was not sufficient justification as compared to "necessity". The ECtHR was also concerned about the inadequate legal safeguards against abuse of the powers by individual officers, because there was no requirement for reasonable suspicion. The Court concluded that the provisions violated article 8(2).

The response to Gillan and Quinton

The Home Secretary, Theresa May, said in a statement on the Judgement on 8 July 2010 that the Government would not have appealed the ECtHR's Judgement:

> The Government cannot appeal this judgment, although we would not have done so had we been able. We have always been clear in our concerns about these powers, and they will be included as part of our review of counter-terrorism legislation.
>
> I can, therefore, tell the House that I will not allow the continued use of section 44 in contravention of the European Court's ruling and, more importantly, in contravention of our civil liberties. But neither will I leave the police without the powers they need to protect us.[155]

The then Shadow Home Secretary, Alan Johnson, criticised the Government's approach:

> The Home Secretary will be aware that the European Court's judgment was based on the way that section 44 powers were used by the Metropolitan police some years ago, and that the previous Government, together with the police authorities, reviewed and improved their procedures in the intervening period. Will she confirm that the number of stop and searches under section 44 has reduced considerably over the last two years? She

---

[152] HM Government, *Review of Counter-Terrorism Powers*, Cm 8004, January 2011, p21
[153] "Police stop and search children as young as two", *Sunday Telegraph*, 16 August 2009
[154] *Case of Gillan and Quinton v. The United Kindom*, (Application no. 4158/05), Strasbourg, 12 January 2010
[155] HC Deb 8 July 2010 c840

> will also be aware that all the UK courts, including the High Court and the House of Lords, rejected the argument that the Gillan and Quinton case represented a breach of article 8. In particular, the Law Lords were doubtful whether an ordinary, superficial search of the person could be said to show a lack of respect for private life. Even if article 8 did apply, they said the procedure was used in accordance with the law and it was impossible to regard a proper exercise of the power as other than proportionate when seeking to counter the great danger of terrorism.
>
> The Home Secretary will also be aware that the Select Committee on Home Affairs examined this issue thoroughly in 2005, when the current Prime Minister was a member of that Committee, and rejected the allegation that the Asian community was being unreasonably targeted by the Metropolitan police in its use of section 44 powers. She will also know that while the independent reviewer of terrorism legislation, Lord Carlile, had concerns that section 44 powers were being used too often - this was before the changes in 2007-08 - he stated clearly that
>
> "the power remains necessary and proportional to the continuing and serious risk of terrorism".
>
> Given all those facts, I am amazed that the Home Secretary would not have pursued an appeal, given that every court in this country rejected the argument in respect of Gillan and Quinton.[156]

As Mr Johnson said, Lord Carlile, then the Government's independent reviewer of terrorism legislation, had indeed argued that the powers were necessary, although he consistently criticised their overuse.[157]

In the statement, Theresa May announced interim guidance pending the conclusion of the Government's review of counter-terrorism legislation. The guidance was in the form of a letter from the Association of Chief Police Officer's lead on terrorism, published on the website of the National Policing Improvement Agency:

> From now on;
>
> • The authorisation test for the use of Section 44 powers will change from being 'expedient' to 'necessary'.
>
> • Officers will no longer be able to stop and search individuals using Section 44 powers but must use those under Section 43, which require the 'reasonable suspicion' threshold.
>
> • Officers will only be able to use Section 44 powers in relation to the searches of vehicles. The Home Office will only confirm these authorisations where they have been considered necessary, and officers will only be able to use the power when they have 'reasonable suspicion'. [158]

The Government's review of counter-terrorism

The Government's review concluded that a power to stop and search individuals and vehicles without reasonable suspicion in exceptional circumstances was operationally

---

156 HC Deb 8 July 2010 c540-1

157 See for example Lord Carlile, *Report on the Operation in 2005 of the Terrorism Act 2000*, 2006, p28 and *Report on the Operation in 2008 of the Terrorism Act 2000* and of part 1 of the Terrorism Act 2006, June 2009, p31

158 See Letter from Craig Mackey, Chief Constable of Cumbria, NPIA website

justified, but it recommended "significant changes" to bring the power into compliance with ECHR rights.[159]

7.6 The Bill's provisions

The Bill would repeal sections 44 to 47 of the *Terrorism Act 2000*. It also amends section 43, which allows the police to search individuals where there is "reasonable suspicion", so that they could use the same power to search vehicles.

Clause 60 and **Schedule 5** would introduce the new power to make searches of vehicles and pedestrians *without* reasonable suspicion. However, in accordance with the Review's recommendations, there are a number of changes compared with the existing provisions:

- The test for authorisation is now that the senior officer must "reasonably expect that an act of terrorism will take place and considers that the authorisation is necessary to prevent the act" (rather than just that the authorisation is "expedient")
- The maximum period of authorisation is reduced from 28 to 14 days
- There are new requirements that the authorisation should last no longer than necessary to prevent an act of terrorism, and that the specified area should be "no greater than necessary"
- The purposes for which the search may be conducted are narrowed; it must be to look for evidence that the vehicle is being used for the purposes of terrorism, or that the person is a terrorist[160]
- The Secretary of State would be able to substitute a more restricted area for the authorisation[161] (as well as the current powers to refuse to confirm the authorisation, to cancel it or to shorten its duration as at present).

Clause 61 would require a specific statutory code of practice to be laid before Parliament and a police officer would have to have regard to this.

Clause 62 and **Schedule 6** amend stop and search powers in Northern Ireland.[162] At present a constable or member of Her Majesty's Forces can stop and search for unlawful munitions and wireless apparatus without reasonable suspicion. The changes would mean that, in future, only the military would be able to do this. The police would generally have to have reasonable suspicion, although there would be similar provisions to the rest of the UK for searches without such suspicion to be authorised for a specific area.

Commentary

The Government's summary of responses to the counter-terrorism review's consultation noted "general acceptance" of the fact that a stop and search power that did not require reasonable suspicion could be necessary in limited circumstances.[163]

Human Rights Watch considers that there is still room for abuse under the new provisions:

---

159 HM Government, *Review of Counter-Terrorism Powers*, Cm 8004, January 2011, paras15-16
160 as defined by section 40(1)(b) of the *Terrorism Act 2000*
161 Schedule 5 paragraph 7
162 Under the *Justice and Security (Northern Ireland) Act 2007*. Details are given in the *Explanatory Notes*, paragraphs 236-255
163 HM Government, *Review of Counter-Terrorism Powers: Summary of responses to the consultation*, Cm 8005, January 2011,

> Though more narrowly drawn and with a higher threshold for authorization and use, the proposed changes would still allow the government to authorize police to stop individuals without any reasonable suspicion of criminal wrongdoing, creating a risk of misuse. Parliament should repeal this power once and for all, and police should rely on powers that require reasonable suspicion.[164]

8 Safeguarding vulnerable groups and criminal records

Part 5 of the Bill would make various amendments to the current law regarding the vetting and barring of individuals who wish to carry out work (paid or voluntary) with children or vulnerable adults. It would also introduce certain procedural changes to the current system for issuing criminal records checks: in particular with regard to the portability of checks and the inclusion of unproven allegations on certificates. Finally, it would introduce a new procedure for people with convictions for certain decriminalised gay sex offences – namely buggery or gross indecency between men – to apply to the Home Secretary to have their convictions disregarded.

8.1 The vetting and barring scheme

The current law

The *Safeguarding Vulnerable Groups Act 2006*, enacted in response to the Bichard Inquiry following the Soham murders, established a vetting and barring scheme in respect of people wishing to undertake "regulated" or "controlled" activities (paid or unpaid) with children or vulnerable adults.[165] The Independent Safeguarding Authority (ISA) was set up to maintain three separate lists: a list of those vetted and registered to undertake regulated or controlled activities; a list of those barred from undertaking regulated or controlled activities with children; and a list of those barred from undertaking such activities with vulnerable adults. Initial estimates were that around 11 million people would be required to register under the scheme once it had been fully implemented.[166] To date, only the barring element of the scheme has been brought into force.

The vetting and barring process

Individuals wanting to undertake regulated activity would have been required to apply to the Criminal Records Bureau (CRB) for registration with the ISA.[167] Upon receiving an application, the CRB would have checked whether the applicant had a criminal record, or whether there was any other relevant information from the police or other sources (e.g. previous employers or professional bodies). If no information was found, the CRB would have informed the applicant that they were ISA-registered and cleared to undertake regulated activity. If relevant information **was** found, the CRB would have passed the application to the ISA for assessment. The ISA would have considered the information and then either registered the individual (if no risk was thought to be posed) or barred them. The registration elements of the vetting and barring scheme have not yet been brought into force.[168]

In addition to barring an individual following an application for registration, the ISA also has the independent ability to bar individuals who come to its notice based on relevant

---

164 *Human Rights Watch, Proposed Counterterrorism Reforms Fall Short*, 11 February 2011

165 See Library Standard Note SN/BT/5255 *Safeguarding vulnerable groups* and Library Research Paper 06/35 *The Safeguarding Vulnerable Groups Bill [HL]* for full background to the 2006 Act. For details of the Bichard Inquiry, see *The Bichard Inquiry Report*, HC 653, June 2004.

166 HC Deb 27 October 2009 c310W

167 ISA website, *Frequently asked questions – How will the new vetting service work?* [on 17 February 2011]

168 The registration elements were due to be phased in from July 2010, but this plan was suspended by the new Government in June 2010 following the general election. The Bill would repeal the registration elements of the scheme in their entirety, leaving only the barring elements in place: see the following sections of this paper.

information from third party sources. The ISA's decision to investigate and potentially bar an individual may be prompted by, for example, referrals from local authorities or professional bodies, details of convictions or cautions, or even information in the media. The ISA has published detailed guidance on the procedure it will follow when considering whether to bar an individual who has come to its attention.[169] Note that convictions for certain offences result in automatic barring, in some cases without any right to make representations.[170] These barring arrangements have been in place since October 2009.[171]

Regulated and controlled activities

The concepts of regulated and controlled activities are defined in the 2006 Act:

> **What is a 'regulated activity'?**
>
> - Any activity of a specified nature that involves contact with children or vulnerable adults frequently, intensively and/or overnight. (Such activities include teaching, training, care, supervision, advice, treatment and transportation.)
> - Any activity allowing contact with children or vulnerable adults that is in a specified place frequently or intensively. (Such places include schools and care homes.)
> - Fostering and childcare.
> - Any activity that involves people in certain defined positions of responsibility. (Such positions include school governor, director of social services and trustee of certain charities.)
>
> 'Regulated activity' is when the activity is frequent (once a month or more) or 'intensive' (takes place on three or more days in a 30-day period).
>
> (...)
>
> **What is a 'controlled activity'?**
>
> - Frequent or intensive support work in general health settings, the NHS and further education. (Such work includes cleaners, caretakers, shop workers, catering staff, car park attendants and receptionists.)
> - Individuals working for specified organisations (e.g. a local authority) who have frequent access to sensitive records about children and vulnerable adults.
> - Support work in adult social care settings. (Such jobs include day centre cleaners and those with access to social care records.)
>
> 'Controlled activity' is when this type of activity is 'frequent' (once a month or more) or 'intensive' (takes place on three or more days in a 30-day period).[172]

The definitions of "frequent" and "intensive" quoted above came under the spotlight in July 2009, after several well known children's authors said that they would no longer be visiting schools in protest at the scope of the scheme:

---

169 ISA, *Guidance Notes for the Barring Decision Making Process*, August 2010

170 *Safeguarding Vulnerable Groups Act 2006 (Prescribed Criteria and Miscellaneous Provisions) Regulations 2009,* SI 2009/37

171 *Safeguarding Vulnerable Groups Act 2006 (Commencement No 6, Transitional Provisions and Savings) Order 2009*, SI 2009/2611

172 Independent Safeguarding Authority factsheet, *Regulated and controlled activities*, October 2007

> Philip Pullman, author of fantasy trilogy His Dark Materials, said the idea was "ludicrous and insulting".
>
> Former children's laureates Anne Fine and Michael Morpurgo have hit out at the scheme which costs £64 per person.
>
> Officials say the checks have been misunderstood and authors will only need them if they go to schools often.
>
> (...)
>
> Anyone who has "regular" or "intense" contact with children or vulnerable adults will by law have to sign up to the Vetting and Barring Scheme from November 2010.
>
> "Regular" is defined as more than once a month and "intense" as three times a month or more, the Home Office says.
>
> The authors, including fantasy writer Mr Pullman, say they have worked in schools for years without ever being left alone with children.
>
> Mr Pullman told BBC Radio 4's Today programme: "It's actually rather dispiriting and sinister.
>
> "Why should I pay £64 to a government agency to give me a little certificate to say I'm not a paedophile.
>
> "Children are abused in the home, not in classes of 30 or groups of 200 in the assembly hall with teachers looking on."[173]

Following this negative publicity, in September 2009 the then Children's Secretary Ed Balls asked the Chair of the ISA, Sir Roger Singleton, to review the definitions of "frequent" and "intensive".[174] Sir Roger's report, *Drawing the Line*, was published on 15 December 2009.[175] One of his recommendations was that the definition of "frequent" should be changed to once a week or more (as opposed to once a month), and "intensive" should be changed to four or more days in one month or overnight (as opposed to three or more days in a thirty day period or overnight).

The Government accepted this recommendation and estimated that its implementation (along with that of Sir Roger's other recommendations) would result in approximately two million fewer individuals needing to register with the ISA.[176] The revised definitions of frequent and intensive were implemented in March 2010.[177]

Developments since the 2010 general election

Following the general election, the Government said that it would be reviewing the vetting and barring scheme and scaling it back to "common sense levels".[178] The first

---

173 "School safety 'insult' to Pullman", *BBC News website*, 16 July 2009

174 Letter from Ed Balls, Children's Secretary, to Barry Sheerman, Chair of the Children, Schools and Families Select Committee, 14 September 2009, DEP 2009-2401

175 Sir Roger Singleton, *'Drawing the Line' – A report on the Government's Vetting and Barring Scheme*, 14 December 2009. The Government's response is set out in a letter from Ed Balls, Children's Secretary, to Sir Roger Singleton, Chief Adviser on Safety of Children, 14 December 2009.

176 HC Deb 14 December 2009 cc 50-53WS

177 The new "intensive" definition was set out in the *Safeguarding Vulnerable Groups Act 2006 (Regulated Activity, Devolution and Miscellaneous Provisions) Order 2010, SI 2010/1154*, while the new "frequent" definition was set out in statutory guidance published in Annex B of the ISA's *Vetting and Barring Scheme Guidance* (March 2010).

178 Cabinet Office, *The Coalition: our programme for government*, May 2010, p20

implementation phase of the vetting elements of the scheme, which was due to commence in July 2010 and would have allowed employees and volunteers to voluntarily apply for registration, was suspended in June 2010 following a statement by Home Secretary Theresa May.[179] This was followed on 22 October 2010 by an announcement setting out the terms of reference for a full review of the vetting and barring scheme:

> In order to meet the coalition's commitment to scale back the vetting and barring regime to common-sense levels, the review will:
>
> Consider the fundamental principles and objectives behind the vetting and barring regime, including;
>
> Evaluating the scope of the scheme's coverage;
>
> The most appropriate function, role and structures of any relevant safeguarding bodies and appropriate governance arrangements;
>
> Recommending what, if any, scheme is needed now; taking into account how to raise awareness and understanding of risk and responsibility for safeguarding in society more generally.[180]

The results of the review were published on 11 February 2011.[181] Its key recommendations were that the barring elements of the scheme that are already in force should be retained, but that the registration elements should be scrapped: "there should be no requirement for people to register with the scheme and there will be no ongoing monitoring".[182] It also recommended that the scope of "regulated activity" be narrowed, and that the concept of "controlled activity" be abandoned altogether. These recommendations have been taken forward in the Bill.[183]

Examples of roles covered by the existing scheme but not by the revised scheme proposed in the Bill:

- Cleaner in an old people's care home
- Sunday school helper
- Medicines counter assistant
- Volunteer parent literacy helper
- Maintenance worker in a children's hospital

Source: Home Office, *Vetting & Barring Scheme Remodelling Review – Report and Recommendations*, February 2011, p18

The Bill's provisions

Chapter 1 of Part 5 of the Bill deals with changes to the vetting and barring scheme. An outline of some of the key clauses is set out below.

Clauses 63 to 65 would restrict the scope of "regulated activity" relating to children and vulnerable adults. In respect of regulated activity relating to children, **clause 63** would amend Part 1 of Schedule 4 to the 2006 Act by narrowing the list of activities covered by the scheme. The list would no longer include activities such as the supervised teaching or instruction of children by a person who is being supervised by another, the provision of legal advice to a child, or paid work that involves the worker having occasional or temporary contact with children (e.g. building contractors who occasionally carry out work on school premises).

Clauses 64 and 65 would restrict the scope of regulated activity relating to vulnerable adults by revising the definitions of both "regulated activity" and "vulnerable adults". Section 59 of

---

179 HC Deb 15 June 2010 cc46-7WS

180 HC Deb 22 October 2010 c77WS. The vetting and barring scheme review was carried out alongside a review of the criminal records system, discussed in the next section of this paper.

181 Home Office, *Vetting & Barring Scheme Remodelling Review – Report and Recommendations*, February 2011

182 Ibid, p4

183 Some of the review's other recommendations will be implemented separately: see Chapter 5 of the Review for details.

the 2006 Act currently defines "vulnerable adult" as someone in a specified setting, for example residential accommodation or sheltered housing, or in receipt of a specified service, for example domiciliary care or any form of health care. Clause 64 would repeal section 59 and redefine "vulnerable adult" as someone in respect of whom a regulated activity was being provided, removing any reference to the setting or the nature of the service. Clause 65 would amend Parts 2 and 3 of Schedule 4 to the Act to restrict the definition of "regulated activity" in respect of vulnerable adults. For example, the 2006 Act currently defines "any form of assistance, advice or guidance provided wholly or mainly for vulnerable adults" as a type of regulated activity. However, the Bill would replace this with "any form of assistance, advice or guidance which relates to an adult's health or care and is provided to an adult who needs it by reason of age, illness or disability".

Clause 66 would amend the eligibility criteria for barring. Under the current system, **anyone** convicted of an offence resulting in automatic barring, or subject to discretionary barring because of other convictions or conduct, could find themselves placed on the barred list regardless of whether they had ever worked with children or vulnerable groups or ever intended to do so. The Bill would amend this by limiting the barring provisions to those individuals who had previously worked, or had expressed an intention to work in, regulated activity. People who had never worked in, or had no intention of working in, regulated activity would no longer be covered by the system and would not be entered on the barred lists even if convicted of a relevant offence.[184]

Clause 67 would abolish the concept of "controlled activity", and **clause 68** would abolishing the registration and monitoring elements of the vetting and barring scheme.

Clause 71 would introduce new arrangements for informing bodies providing regulated activities about whether a person is barred. Two options would be available: reactive and proactive. The reactive option would enable a regulated activity provider to apply to the ISA to find out whether a particular person is barred. Under the proactive option, the regulated activity provider could register with the ISA to be automatically informed if a particular person becomes barred. Both options would require the consent of the individual in question.

Clause 72 would make it a requirement for a regulated activity provider to check whether a person is barred before permitting him or her to engage in regulated activity.

Volunteering England has said that it "welcomes the broad proposals" set out in the Bill, and that they will "reduce a significant barrier to volunteering".[185] However, other groups are concerned that the proposed reforms may put children and vulnerable adults at greater risk. For example, the Churches' Child Protection Advisory Service, a Christian child protection charity, has said that the Bill "will make it easier, not harder, for unscrupulous sexual predators to abuse in churches".[186]

8.2 Criminal records

Chapter 2 of Part 5 of the Bill would make a number of changes to the current system for criminal records checks. The results of checks would no longer be sent directly to employers, enabling individual applicants to check and (if necessary) dispute the results of

---

[184] Note that if such a person did decide at some point in the future to apply to work or volunteer in a regulated activity, their prospective employer would be required to check their barred status. This would be done by way of an enhanced criminal records check – the person would be required to indicate on the application for this check that they were intending to work in a regulated activity, at which point the new provisions in the Bill would kick in (the person having expressed an intention to work in regulated activity) and the person could be added to the barred list.

[185] Volunteering England news release, *Freedom Bill announcement on safeguarding*, 11 February 2011

[186] CCPAS press release, *New VBS regulations will make it easier for sexual predators to abuse in churches, says CCPAS*, 11 February 2011

checks before forwarding them to employers. The Bill would also amend the test to be used by the police when deciding whether to include non-conviction information on an enhanced criminal records check. A new procedure for updating checks on a continuous basis would also be introduced in an effort to make checks more "portable".

The current law

An individual who is convicted of a recordable offence has a "nominal record" of that conviction placed on the Police National Computer (PNC). Nominal records are also created for individuals who are cautioned or arrested for such offences. The review, retention and disposal of nominal records on the PNC is governed by Retention Guidelines prepared by the Association of Chief Police Officers (ACPO).[187] An individual's nominal record is retained until his 100th birthday and can be disclosed as part of a criminal records check.[188]

In addition to conviction information held on the PNC, police forces also hold non-conviction information on local systems. Non-conviction information may include, for example, details of acquittals, unproven allegations or details of criminal investigations that did not lead to charges.

Both conviction and non-conviction information is capable of being disclosed to prospective employers as part of a criminal records check. Two levels of criminal records check, standard and enhanced, are currently available from the Criminal Records Bureau (CRB):

> **Standard Check**
>
> Standard checks can be applied for by people entering certain professions, such as members of the legal and accountancy professions and applying for specified licences. A Standard check contains:
>
> - details of all convictions, cautions, reprimands and warnings held on the Police National Computer (PNC)
>
> A Standard check cannot reveal if a person is ISA- registered or barred from working with children or vulnerable adults.
>
> **Enhanced Check**
>
> An Enhanced Disclosure is available to anyone who works in what is known as a "prescribed position". These are the positions which are in the ROA and have also been named in Police Act Regulations. Regulated Activity with either Children or Vulnerable Adults, certain Judicial Appointments and Gambling Licence Applications are examples of prescribed positions.
>
> Enhanced CRB checks contain the same information as the Standard Disclosure but with the addition of;
>
> - any relevant and proportionate information held by the local police forces.
> - a check of the new Children and or Vulnerable Adults barred lists where requested.[189]

---

187 ACPO, *Retention Guidelines for Nominal Records on the Police National Computer*, March 2006

188 The Court of Appeal has ruled that this retention policy is lawful and does not infringe data protection legislation: *Chief Constable of Humberside Police & Ors v The Information Commissioner & Anor* [2009] EWCA Civ 1079

189 CRB website, *The Disclosure Service* [on 21 February 2011]

Guidance on the factors the police should consider when deciding whether non-conviction information is relevant and proportionate and should be included on an enhanced disclosure is currently set out in Home Office Circular 5/2005 *Criminal Records Bureau: local checks by police forces*. The police will also refer to an internal Quality Assurance Framework:

> The Quality Assurance Framework (QAF) is a standardised approach to processing local intelligence information held by Police Force Disclosure Units and was developed by the Association of Chief Police Officers (ACPO) and the CRB. QAF provides a step-by-step process framework that ensures that information is considered consistently and in the same way every time. Searches performed on local systems using the QAF Framework and document set produce an audit trail that can be used for quality assurance and to assure QAF compliance.[190]

There have been a number of judicial review challenges to the inclusion of non-conviction information on enhanced disclosures. Until October 2009, the leading case on the disclosure of police information in connection with an enhanced disclosure was *R (on the application of X) v Chief Constable of the West Midlands Police and another* [2005] 1 All ER 610, in which the Court of Appeal held that the policy of the relevant legislation, in order to serve the pressing social need to protect children and vulnerable adults, was that the information should be disclosed to the CRB by the police even if it only "might" be true.

However, in October 2009 the Supreme Court ruled that equal weight should be given to the human rights of the person applying for the enhanced disclosure as to the need to protect children and vulnerable adults; following *R (X) v Chief Constable of the West Midlands Police* the balance had tipped too far against the applicant.[191] The Supreme Court held that all enhanced disclosures are likely to engage Article 8 of the European Convention on Human Rights (right to respect for private life), as the information has been collected and stored in police records and disclosure of relevant information is likely to diminish the applicant's employment prospects. The police should apply a two-stage analysis when deciding whether to disclose non-conviction information: first, is the information reliable and relevant; and second, in light of the public interest and the likely impact on the applicant, is it proportionate to disclose the information. Factors to be considered in assessing proportionality should include the gravity of the information, its reliability and relevance, the applicant's opportunity to rebut the information, the period that has elapsed since the relevant events, and the adverse effect of the disclosure.

The Supreme Court went on to state that if the chief constable is not satisfied that the applicant has had a fair opportunity to answer any allegations in the information concerned, or if the information is historical or vague or he has doubts as to its potential relevance, the applicant should be given the chance to make representations as to why it should not be included.

---

[190] HC Deb 27 January 2010 cc913-4W. The Quality Assurance Framework is available from the CRB's website. The most relevant documents in relation to the disclosure of unproven allegations are *MP7a and 7b: Disclosure rationale and method* (version 7, last updated 13 November 2009) and *MP8: Chief officer/delegate guidelines* (version 7, last updated 22 November 2009). The CRB has also published a guidance document entitled *QAF Guide – ACPO* (December 2009), which sets out "the thinking on which QAF MP8 is based".

[191] *R (L) v Commissioner of Police of the Metropolis* [2009] UKSC 3. The Supreme Court has also published a press summary of the decision, which provides an overview of the key issues set out in the judgment.

Developments since the 2010 general election: the Home Office review

Following the general election, the Government said that it would "review the criminal records and vetting and barring regime and scale it back to common sense levels".[192] The review was conducted by Sunita Mason, the Government's Independent Advisor for Criminality Information Management.[193] Terms of reference were announced by the Home Secretary on 22 October 2010.[194]

Ms Mason's report into phase 1 of her review was published on 11 February 2011.[195] She said that her recommendations, listed to the right, would "ensure that public protection is maintained whilst individual civil liberties are better defended". The Government has not yet published a formal response, but is proposing to take forward a number of Ms Mason's recommendations in the Bill.

Recommendations from Phase 1 of the review:

1. Eligibility for criminal records checks should be scaled back.

2. Checks should be portable between jobs and activities.

3. The CRB should introduce an online system to allow employers to check if updated information is held on an applicant.

4. A new CRB procedure should be developed so that the criminal records certificate is only issued directly to the individual applicant.

5. The Government should introduce a filter to remove old and minor conviction information from criminal records checks.

6. A package of measures to improve the disclosure of police information to employers should be introduced.

7. The CRB should develop an open and transparent representations process, and disclosure of police information should be overseen by an independent expert.

8. Penalties and sanctions should be rigorously enforced where employers knowingly make unlawful criminal records check applications.

9. Basic level criminal records checks should be introduced in England and Wales.

10. Comprehensive and easily understood guidance explaining the criminal records and employment checking regime should be developed.

The Bill's provisions

Clause 77 of the Bill would amend the procedure for issuing a criminal records certificate following a check. At present, the CRB dispatches two copies of the certificate once a check has been completed: one to the individual applicant, and the other to the body that requested the check (e.g. a prospective employer). In her review, Ms Mason identified a number of difficulties with this parallel disclosure,[196] in particular the fact that there is no opportunity for the individual applicant to challenge any of the information on the certificate **before** it is seen by a potential employer. She therefore recommended that certificates should only be sent to the individual applicants, who would then be able to decide when and whether to forward the certificate to a potential employer. Any risk of individuals tampering with their certificates would be dealt with by "IT solutions". Clause 77(a) would implement this recommendation.

---

192 Cabinet Office, *The Coalition: our programme for government*, May 2010, p20

193 Ms Mason was appointed by the Labour Government in 2009. She conducted an independent review of the criminal records system for the then Home Secretary Alan Johnson, which was published in March 2010: see Home Office, *A Balanced Approach – Independent Review by Sunita Mason*, March 2010 (DEP 2010-0745).

194 HC Deb 22 October 2010 c78WS

195 Sunita Mason, *A Common Sense Approach – Report on Phase 1*, February 2011

196 Ibid, pp24-27

Ms Mason also recommended that the current procedure under section 113B of the *Police Act 1997*, which allows the police to disclose sensitive non-conviction information to a prospective employer by way of a side letter rather than on the face of the certificate, should be abolished.[197] She said that the police should instead use other methods to assess and, where appropriate, disclose such information, for example under the Multi-Agency Public Protection Arrangements (MAPPA) or by using their common law powers to prevent crime and protect the public. Clause 77(b) would give effect to the recommendation to abolish the relevant provisions of section 113B of the 1997 Act.

Clause 78 would introduce a new requirement for applicants for criminal records checks to be aged 16 or over. This reflects Ms Mason's recommendation that children should not be eligible for criminal records checks:

> Another eligibility concern is that criminal records checks are currently conducted on children. In 2009/10 just over 5,000 checks were issued in respect of applicants under the age of 16. There are obvious civil liberty considerations in carrying out checks on children. Common sense dictates that they should not be left unsupervised in a position of authority with other children or vulnerable adults.[198]

Clause 79 would implement a number of Ms Mason's recommendations relating to the current police procedure for disclosing non-conviction information as part of an enhanced criminal records check.[199] At present, the police can disclose such information where, in the opinion of the chief officer, it "might be relevant".[200] Clause 79 would substitute a more specific threshold of "reasonably believes to be relevant".

Decisions as to relevancy are currently made locally by the chief officer of the force that holds the information concerned. However, Ms Mason recommended that chief officers be given the power to make relevancy decisions on information held by other forces as well as their own:

> Work is now well advanced to provide centralised access to police intelligence via the Police National Database and all forces should be using the first phase of this system by the middle of 2011. The Police National Database essentially means that all police information held will be visible to all forces rather than only being placed on a local system and visible only to officers in that force.
>
> The introduction of the Police National Database provides a great opportunity to use improved technology and business processes for handling police information to enhance CRB disclosure arrangements.
>
> Effectively, one Chief Officer could access police information from a number of forces via the Police National Database and make the entire set of relevancy decisions on behalf of the service as a whole. Potentially this is a much quicker, efficient and consistent approach and ought to deliver a service of improved quality.[201]

Clause 79 would implement this recommendation. It would also implement Ms Mason's recommendation for a statutory code of practice for chief officers to follow when deciding whether to disclose non-conviction information, which she considered was necessary to

---

197 Ibid, pp36-37. The power is generally used in respect of information that might place others at risk or jeopardise an ongoing investigation if the applicant was aware of it.
198 Ibid, p19
199 Ibid, pp30-39
200 *Police Act 1997*, s113B(4)
201 Sunita Mason, *A Common Sense Approach – Report on Phase 1*, February 2011, pp37-38

"strengthen" the Quality Assurance Framework that the police currently use.[202] Clause 79 would also enable individual applicants to request a review of any non-conviction information included in an enhance check. The review would be conducted by a chief officer, although the Explanatory Notes suggest that in practice this would be a different chief officer from the one who made the original decision to disclose the information.[203]

Clause 80 would implement Ms Mason's third recommendation, which was that an online system should be introduced to enable employers to check if updated information is held on an individual:

> I envisage a simple online system whereby an employer, with the consent of the applicant, can confirm the details contained on a criminal records certificate. If there has been a change since the certificate was issued, the employer will be prompted to request a new check. If there is no new information it will simply indicate there is no change.
>
> As previously stated, the result of the vast majority of repeated checks will show no change. Only at the point where an online check indicates that there is new information would a fresh disclosure application be required.[204]

Individuals who wanted to make use of the new updating system would be required to subscribe to it on an annual basis. A fee would be payable; it would be prescribed by regulations and would be "set at a level necessary to recover the costs of the service". The Government considers that the cost of subscribing would be offset by the removal of the need to make repeat applications for a criminal records certificate.[205]

The Scout Association, which carries out more criminal records checks than any other single voluntary organisation, has said that the proposed scheme "has much to recommend it" but has also raised a number of concerns:

> We are pleased that the Government has recognised that many volunteers do so in a number of different capacities and has made provision for CRB checks to be portable. This will be welcomed by our many volunteers who often offer a significant amount of their time to support numerous charitable organisations.
>
> However, we fear that the proposed changes to criminal record checks will add to the burden faced by voluntary organisations such as the Scouts.
>
> The decision to send a single copy of the CRB disclosure to a potential volunteer who must then pass it to their local Scout leader will undoubtedly save the Government money but it will increase the amount of bureaucracy expected of local volunteers, who give their time to support young people not to chase CRBs. We call on the Government to retain a system where a copy of the CRB disclosure is sent direct to the organisation to ensure that local volunteers remain free to do what they do best, unfettered by unnecessary bureaucracy.
>
> We accept the concern that in some cases this might mean that incorrect information could be disclosed to voluntary organisations before an individual has a right to redress, however we believe that a seven day delay could be introduced between the individual and the registered body receiving the CRB check. This would allow a person

---

202 See footnote 190 above
203 *Explanatory Notes*, paragraph 301
204 Sunita Mason, *A Common Sense Approach – Report on Phase 1*, February 2011, p23
205 *Explanatory Notes*, paragraph 303

> the opportunity to check and appeal any inaccurate information without tying existing volunteers on the ground up in bureaucratic knots.[206]

8.3 Disregarding convictions for historic consensual gay sex offences

Chapter 3 of Part 5 of the Bill would enable men with old convictions for certain gay sex offences that are now decriminalised to apply to the Home Secretary for their deletion. If deleted, the offences would no longer be disclosed on criminal records checks and the individuals concerned would be treated as if they had never committed or been convicted of the offences in question.

Background

Under sections 12 and 13 of the *Sexual Offences Act 1956*, which set out the offences of buggery and gross indecency between men, consensual homosexual sex between men over the age of consent was criminalised.[207] Decriminalisation of consensual sex between men over the age of 21 took place in 1967.[208] The age of consent was lowered to 18 in 1994 and again to 16 in 2000.[209] However, any convictions predating the decriminalisation of consensual gay sex and the lowering of the age of consent will currently form part of an individual's criminal record and can be disclosed to potential employers as part of a criminal records check. The Home Office estimates there are approximately 50,000 convictions for section 12 or 13 offences recorded on the Police National Computer, of which approximately 16,000 relate to consensual sexual activity between men aged 16 or over.[210]

Following the 2010 general election, the Government said that it would be legislating for historical convictions for consensual gay sex between men aged 16 or over to be treated as spent, meaning they would no longer show up on criminal records checks.[211]

The Government's Equality Strategy, published in December 2010, set out further details:

> We will ... change the law so people with historical convictions for consensual gay sex with over 16s can apply for their record to be deleted from the Police National Computer, ensuring it no longer has to be declared and will not show up on criminal record checks.[212]

Equalities minister Lynne Featherstone said:

> It is totally unfair and unjust that men who have a conviction for something that has long not been illegal should have to fear that being exposed-and exposed to partners they live with, who may not know. Such men will never again have to disclose that information. I hope very much that those gay men whom that has inhibited from volunteering will now find that inhibition removed.[213]

The Bill's provisions

The Bill would introduce a scheme whereby men with convictions or cautions under sections 12 or 13 of the 1956 Act, and the corresponding earlier offences under the *Offences Against*

---

206 Scout Association press release, *Government plans to scale back vetting and barring scheme*, 11 February 2011

207 Corresponding earlier offences were set out in section 61 of the *Offences Against the Person Act 1861* and section 11 of the *Criminal Law Amendment Act 1885*.

208 *Sexual Offences Act 1967*, s1

209 *Criminal Justice and Public Order Act 1994*, s143 and *Sexual Offences (Amendment) Act 2000*, s1

210 Home Office, *Equality Impact Assessment - Removal of decriminalised offences for consensual gay sex from the Police National Computer*, 21 December 2010, p2

211 Cabinet Office, *The Coalition: our programme for government*, May 2010, p24

212 HM Government, *The Equality Strategy – Building a Fairer Britain*, December 2010, p21

213 HC Deb 2 December 2010 c961

the Person Act 1861 and the *Criminal Law Amendment Act 1885*, could apply to the Home Secretary to have their convictions or cautions "disregarded".

Clause 82 would require the Home Secretary to be satisfied that the following conditions had been met before disregarding a conviction or caution:

- the other person involved in the conduct constituting the offence consented to it and was aged 16 or over; and
- any such conduct now would not be an offence under section 71 of the *Sexual Offences Act 2003* (sexual activity in a public lavatory).

The aim of these two conditions is to ensure that the only convictions disregarded are those for behaviour that is no longer criminal. As set out in the Explanatory Notes, some of the conduct covered by sections 12 and 13 is still criminal today, and so should not be capable of being disregarded:

> As well as consensual gay sex with a person over the age of consent, the offence in section 12 of the 1956 Act also encompasses non-consensual buggery, bestiality and under-age buggery, and the section 13 offence also includes gross indecency with somebody under the age of consent, all of which remains criminal behaviour today.[214]

Clause 83 sets out the procedure for applying to the Home Secretary for a conviction to be disregarded. Applications must be in writing and include details of the conviction or caution, and may also include representations by the applicant or written evidence about the two conditions referred to above.

In coming to a decision as to whether to disregard a conviction or caution, **clause 84** would require the Home Secretary to consider any representations or evidence included in the application, together with any available record of the investigation of the offence and any relevant proceedings relating to it. No oral hearings would be held.

Under **clause 85**, following a successful application to disregard a conviction or caution, the Secretary of State would direct the "relevant data controller"[215] to delete details of the conviction or caution from "relevant official records".[216] The Home Secretary would be given order-making powers (subject to the negative resolution procedure) to amend the definitions of "relevant data controller" and "relevant official records". Note that clause 85(5) would define "delete" as follows:

> "delete", in relation to such official records as may be prescribed, means record with the details of the conviction or caution concerned –
>
> (a) the fact that it is a disregarded conviction or caution, and
>
> (b) the effect of it being such a conviction or caution.

Under **clause 86**, a person with a disregarded conviction or caution would be treated for all purposes in law as if he had not committed the offence, or been charged with, prosecuted for, convicted of, sentenced for or cautioned for it.

---

214 *Explanatory Notes*, paragraph 308

215 Usually the chief officer of police of the force that investigated the offence: *Explanatory Notes*, paragraph 317

216 Namely the names database held by the National Policing Improvement Agency for the use of constables, and such other official records as may be prescribed.

Details of disregarded cautions and convictions could not be used in judicial proceedings. In addition, questions about previous convictions put to a person in any other context (for example by a prospective employer) would be treated as not relating to any disregarded conviction or caution.

Clause 87 would preserve the existing power of the Queen, under the Royal prerogative, to issue a free pardon, quash a conviction or sentence, or commute a sentence. These actions would therefore still be available in respect of disregarded convictions or cautions despite the operation of clause 86.

Clause 89 would give unsuccessful applicants the right to appeal the Home Secretary's refusal to disregard a conviction or caution to the High Court. The High Court would only be able to consider the evidence that had been available to the Home Secretary, so new evidence could not be introduced at this stage. There would not be any further appeal from the High Court's decision.

Under **clause 90**, the Home Secretary would be able to appoint persons to advise on whether the conditions required for a disregard had been met.

The Lesbian & Gay Foundation said:

> **The Lesbian & Gay Foundation welcome this part of the new Freedom Bill** and would like to encourage all those who have been affected by historic convictions to apply to get them removed if they have been unable to apply for jobs and voluntary roles because of the fear that these historic and unjust convictions would be revealed through criminal record checks.
>
> For many people these convictions have had an incredibly negative effect on their lives long after the offences they were convicted for were removed from the statute books.[217]

Ben Summerskill, chief executive of the charity Stonewall, said:

> For some gay men, these convictions have continued to overshadow their lives long after the offences were removed from the statute book. Britain has moved on. It's only right that these men should be free to apply for jobs and voluntary roles without fearing that these historic and unjust convictions will be revealed through criminal record checks. Stonewall will be encouraging politicians of all parties to back the measures in the months ahead.[218]

9 Freedom of Information and Data Protection

9.1 Duty to publish datasets

The Conservatives published a Conservative Technology Manifesto in March 2010,[219] signalling a commitment to a new Right to Data policy, similar to that introduced in the United States by President Obama. This would enable the public to request and receive government datasets, thereby improving accountability to the public and also creating economic value by building innovative applications and services that make use of government data.

The Coalition Agreement of 11 May 2010 promised extensions to the *Freedom of Information Act 2000* and more transparency. In May 2010 David Cameron required departments to

---

[217] Lesbian & Gay Foundation, *Historical gay convictions to be removed*, 11 February 2011
[218] Stonewall press release, *Stonewall welcomes erasing of unjust convictions in Freedom Bill*, 11 February 2011
[219] Conservative Party news, *Conservative technology manifesto launched*, 11 March 2010

publish data in an open-source format so it could be reused by third parties. He established a Public Sector Transparency Board in the Cabinet Office, chaired by the Minister for the Cabinet Office, Francis Maude.

David Cameron spoke on 8 July 2010 of the need to 'turn government on its head' by making departments accountable to the public through the release of information. Over 5,300 datasets have been released.[220] Some of these are new and some have been published before. These do not contain personal data and so do not engage the *Data Protection Act 1998.*

People who want to re-use public sector datasets often complain of being given datasets in a form that makes them difficult to re-use – for example tables on paper, in a pdf document or shown in a picture. Datasets generally need be in a spreadsheet or database format to be reused easily. Converting the text into such a format may require considerable time and effort, especially where datasets are large – a dataset may contain hundreds or thousands of individual data items (for example numbers or pieces of text).

Clause 92 amends section 11 of the *Freedom of Information Act 2000* (FoI) to require public authorities to release information that is, or forms part of, a dataset in an electronic form capable of re-use, where requested to do so. This would appear to be to prevent data being presented in pdf format only. The term dataset is defined so that it is:

- not capable of including the 'product of analysis or interpretation, other than calculation' and is
- not an official statistic 'within the meaning of section 6(1) of the *Statistics and Registration Service Act 2007'* and
- not presented in a way that has been organised or altered since obtained or recorded. This means that the data is "raw" in form. One point to consider is that reference to sorting the data in some way might stop a dataset having to be released in a re-usable form.

It is worth noting that official statistics are already subject to a regime set out in the *Statistics and Registration Service Act 2007*.[221] The *Code of Practice for Official Statistics* goes beyond the requirements for the release of datasets in Clause 92, for example setting out that producers of official statistics should ensure that official statistics are disseminated in forms that enable and encourage reuse. The stronger requirements for official statistics reflect their wider intended purpose. Official statistics and official statistics datasets should be designed in a way that takes user needs into account – allowing them to inform decision-making by government, public services, business, researchers and the public. Other public sector datasets will often have been designed for specific administrative purposes without the expectation that they might be re-used outside their original setting. They may come with little explanation – it may be difficult to understand how the datasets can be used and what their limitations are.

In addition, the publication scheme must include a requirement to publish any dataset subject to a request and to republish any updated version of the dataset. The *Explanatory Notes* explain that there is no absolute duty to provide datasets in a re-useable format as "there may be practical difficulties in relation to costs and IT to convert the format of the

---

[220] at http://data.gov.uk/data

[221] Official statistics are statistics that are produced by Crown bodies and certain other bodies specified by order – these are typically public bodies with a national reach

information".[222] No impact assessment has been produced for this part of the Bill, and so it is not possible to quantify the potential costs to public authorities. Some guidance may be necessary to assist public bodies. It would be possible for a requester to appeal to the Information Commissioner if dissatisfied with the response of the body.

Clause 92 also adds a new section 11A. This creates a new duty on public authorities to make a dataset available for re-use in accordance with the terms of the specified licence, thereby making the copyright regime more liberal.

9.2 Publicly owned companies and FoI

When the FoI legislation was passed, sections 4 and 5 allowed for more bodies to be covered by the duty to supply information. Section 4 allowed the Secretary of State to amend Schedule 1 by order to add new or additional public bodies. Section 5 allowed the Secretary of State to designate as a public authority bodies carrying out functions of a public nature or providing public services for a public authority. Section 6 provides that publicly owned companies, if wholly owned by the Crown or a public authority, are covered by FoI.

The Ministry of Justice undertook a consultation in 2008-9 on the question of designating companies and other bodies under section 5 of the FoI Act. The analysis of the responses is available online. The then Minister, Michael Wills, announced on 16 July 2009 that the Government planned to bring the Association of Chief Police Officers (ACPO), the Financial Ombudsman Service and the Universities and Colleges Admission Service (UCAS) within FoI by bringing forward a section 5 order under that Act. Subsequently, on 30 March 2010 in a written ministerial statement, Mr Wills promised to issue a section 5 order in relation to these organisations in the next parliamentary session.[223] The general election intervened.

The new Government continued the general policy objectives. Academies were brought within FoI as part of the *Academies Act 2010*.[224] On 7 January 2011, the Ministry of Justice issued a press release on extension of FoI rights among a package of announcements on transparency.[225] On 18 January 2011, Kenneth Clarke promised in a written ministerial statement that there would be a section 5 order and further consultation:

> We will introduce a section 5 order under the Freedom of Information Act in the spring to bring the Association of Chief Police Officers, the Financial Ombudsman Service and the University and Colleges Admissions Service within the Act's scope.
>
> We will also consult a range of further bodies with a view to their inclusion in the Act by a further section 5 order later this year. This includes bodies as diverse as Examination Boards, Harbour Authorities, the Local Government Association and the NHS Confederation.
>
> We will amend section 6 of the FOI Act in the Freedom Bill to end the anomaly where companies wholly owned by a single public authority are subject to the Act but those wholly owned by more than one public authority are not. We will also introduce measures to enhance the independence of the Information Commissioner's Office in the same Bill.[226]

Clause 93 provides that companies which are wholly owned by one or more bodies from the wider public sector are covered by FoI.

---

[222] Protection of Freedoms Bill - Explanatory Notes, para 334
[223] HC Deb 30 March 2011 c111WS
[224] Para 10 of Schedule 2
[225] Ministry of Justice news release, *Opening up public bodies to public scrutiny*, 7 January 2011
[226] HC Deb 18 January 2010 c35WS

Clause 94 extends to Northern Ireland amendments made in the *Constitutional Reform and Governance Act 2010* (CRAG) which make exempt from FoI communications with the royal family or the royal household. It also extends to Northern Ireland the changes made to historical records in CRAG, which introduced a new 20 year rule, instead of 30. Further background is available in Library Standard Note SN/PC/5377 *Public records, freedom of information and the royal family*.

9.3 Independence of the Information Commissioner

The office of Information Commissioner was established by the *Freedom of Information Act 2000,* which amended Schedule 5 of the *Data Protection Act 1998.* The Commissioner took over the functions of the Data Protection Commissioner and was given a role as an independent regulator with respect to FoI. The role of the Commissioner is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.[227]

The Commissioner is appointed by the Secretary of State for Justice, but can only be dismissed following addresses from both Houses. This follows the precedent used for other independent officials, such as senior judges, the Comptroller and Auditor General, and the Electoral Commission. Further information is available in Library Standard Note SN/PC/4720 *Officers of Parliament: Recent Developments*. The budget for the Commissioner's office is taken from a departmental vote, and not from the consolidated fund, unlike the National Audit Office and the Electoral Commission. The salary of the Information Commissioner itself is funded from the standing services of the consolidated fund and he is appointed by letters patent.

The Justice Select Committee (formerly the Constitutional Affairs Select Committee) has recommended for some years that the independence of the Information Commissioner be bolstered. It has questioned whether it was appropriate for the Ministry of Justice to set the budget of an independent regulator.[228] In February 2009, the Committee carried out a pre-appointment hearing in respect of the incoming Information Commissioner, Christopher Graham. The report commented:

> In our previous form as the Constitutional Affairs Committee we recommended that the Information Commissioner should be directly responsible to, and funded by, Parliament. The Government's position has been that, in its view, the status quo provided for independent decision-making by the Commissioner while permitting the proper scrutiny of public resources.
>
> Mr Thomas, the current Commissioner, told us that direct funding from Parliament was "in principle … the right approach" citing the position of the Scottish Commissioner who is funded by, and accountable to, the Scottish Parliament. Mr Thomas emphasised the constructive relationship between his office and the Ministry of Justice (MoJ) but pointed to the potential for "perception issues" arising from the fact that his funding came from the MoJ's Information Directorate, which also housed the team of officials providing advice to all government departments on freedom of information cases and issues. He described this as "a slightly uncomfortable situation". Mr Graham was cautious. While recognising that this Committee had made "the running" with this

[227] ICO website, *About the Information Commissioner's Office,* February 2011
[228] *Constitutional Affairs Select Committee Seventh Report 2005-6 Freedom of Information: One Year On*, HC 991, June 2006

> recommendation, he confined himself, at this early stage, to saying that the proposition seemed "logical" and that he "would not resist it".[229]

In the foreword to his first annual report as Commissioner, Mr Graham made the case for a change in governance structure so that it was "suitable for an independent public official whose accountability is fully to Parliament rather than primarily via a Department of State....I believe that the ICO has not just to be independent of government but seen to be independent in its reporting and funding arrangements."[230]

On 16 February the junior Justice Minister, Jonathan Djanogly, announced that there would be a pre-appointment hearing process with a veto for the select committee:

> The Government will strengthen the role of Parliament in the appointment of the next Commissioner in 2014. For this appointment, the Government will offer the Justice Select Committee a pre-appointment hearing with the preferred candidate and will accept the Committee's conclusion on whether or not the candidate should be appointed. This will make the appointment process more open and transparent and enhance the independence of the office. [231]

However, this is not set out as a statutory right in the Bill, unlike the position with the Chair of the Office for Budget Responsibility in Schedule 1 of the *Budget Responsibility and National Audit Bill [HL]* where the appointment can only be made with the consent of the Treasury Committee.

Clause 95 introduces a series of refinements to Schedule 5 of the *Data Protection Act* to ensure the appointment and dismissal process is fair and transparent. It makes an adjustment in the process of moving an address in respect of removal from office. An address would be sought only if a minister is satisfied that one of a new list of grounds is satisfied. These grounds include failure to discharge functions or bankruptcy or conviction for a criminal offence.

The clause also amends Schedule 5 so that the Commissioner is appointed on merit and on the basis of fair and open competition. The Commissioner would only be able to be appointed for a single fixed term and would no longer be required to resign when reaching 65. These changes reflect the general trend towards

Reactions to the FoI changes

Information Commissioner, Christopher Graham, said:

> "I welcome the publication of the Protection of Freedoms Bill and support its aims of strengthening privacy, delivering greater transparency and achieving improved accountability, as well as greater independence for the ICO.

The Campaign for Freedom of Information said:

> Requiring public authorities to publish data sets proactively, under the 'publication schemes' that all authorities are required to have under the Act, was a positive step, the Campaign said. It was also helpful that when applying for datasets applicants would be entitled to specify that they be released in a reusable electronic format. The Campaign said that should prevent authorities deliberately turning a spreadsheet into a pdf, before releasing it, to stop requesters running their own analyses of the spreadsheet itself. ...
>
> The new Bill also seeks to prevent authorities invoking copyright to prevent requesters republishing datasets released under the Act, where the authority is the copyright holder. The Campaign said this was a positive step which should be extended beyond datasets. Authorities frequently insist that requesters apply to them for a copyright license to reproduce information about the authorities' own policies and performance. It said this was an unnecessary restriction which obstructs the use of information which has no commercial value to the authorities themselves.

---

229 Justice Committee, *The work of the Information Commissioner: appointment of a new Commissioner*, HC 146 2008-09, paras 29-30

230 Information Commissioner Annual Report 2010, July 2010

231 HC Deb 16 February 2011 c87-88WMS

single term appointments for constitutional watchdogs as a method of ensuring continued independence.

Clause 96 removes the current requirement that certain guidance issued by the Commissioner must be approved by the Secretary of State. **Clause 97** removes the current requirement for the Information Commissioner to seek consent from the Secretary of State before making charges for services. **Clause 98** removes the current requirement to obtain the approval of the Secretary of State for the number of staff to be employed by the Commissioner and requires the Commissioner to have regard to selection on merit on the basis of fair and open competition.

However, the clauses do not offer the Information Commissioner independence in terms of the budget for the office, and there is likely to be further pressure to achieve this during the passage of this Bill.

9.4 Reactions to the FoI changes

Information Commissioner, Christopher Graham, said:

> I welcome the publication of the Protection of Freedoms Bill and support its aims of strengthening privacy, delivering greater transparency and achieving improved accountability, as well as greater independence for the ICO. [232]

The Campaign for Freedom of Information said:

> Requiring public authorities to publish data sets proactively, under the 'publication schemes' that all authorities are required to have under the Act, was a positive step, the Campaign said. It was also helpful that when applying for datasets applicants would be entitled to specify that they be released in a reusable electronic format. The Campaign said that should prevent authorities deliberately turning a spreadsheet into a pdf, before releasing it, to stop requesters running their own analyses of the spreadsheet itself. ...
>
> The new Bill also seeks to prevent authorities invoking copyright to prevent requesters republishing datasets released under the Act, where the authority is the copyright holder. The Campaign said this was a positive step which should be extended beyond datasets. Authorities frequently insist that requesters apply to them for a copyright license to reproduce information about the authorities' own policies and performance. It said this was an unnecessary restriction which obstructs the use of information which has no commercial value to the authorities themselves. [233]

10 Fraud trials without a jury

Section 43 of the *Criminal Justice Act 2003* would have enabled the prosecution in certain serious and complex fraud cases to apply for the trial to be conducted without a jury. Background to this provision, and the other provisions in the 2003 Act dealing with jury trials, is set out Library Research Paper 02/73 *The Criminal Justice Bill: Juries and Mode of Trial*. The 2003 Act's jury provisions proved particularly controversial during the Act's passage through Parliament, and section 43 was only accepted after the Government agreed that it would not be implemented without an affirmative resolution of both Houses:

> ... the overall mood (including that of most former judges and practitioners) was hostile to a set of provisions which were seen as objectionable in principle and as being the

---

[232] ICO Statement 11 February 2011 "ICO response to Protection of Freedoms Bill"
[233] "Welcome for Freedom Bill's FoI changes" 11 February 2011 Campaign for Freedom of Information

> thin end of the wedge even though they may not at this stage impact on a large number of trials. The mood was undoubtedly partly influenced by the fact that the provisions were seen as part of a continuing strategy of the government to restrict the role of the jury, a strategy with which the House had in recent years done battle in rejecting two Mode of Trial Bills which sought to limit the defendant's right to elect Crown Court trial for indictable offences.
>
> Having been removed from the Bill in the Lords in July, the non-jury trial proposals reappeared only when the Bill returned to the Commons for consideration of Lords amendments at the very end of its passage when the government reinstated the provisions which meant that they had to go back to the Lords for their approval. As a result, the Bill went backwards and forwards in the final days and hours of the parliamentary session as the government and those opposed to the provisions tested each other's nerve. The government was in danger of losing the Bill altogether although it made it clear finally that it would be prepared to extend the parliamentary session into the following week (during which the Queen's Speech at the start of the new session was due) in order to get the Bill passed in an acceptable form. Eventually ... the Act was passed with hours to spare within the original time frame, with two out of the three main provisions on non-jury trial in place but without the third provision. That is with no provision for defendants to opt for non-jury trial and with one of the other two provisions, complex frauds, emasculated by a commitment not to implement without an affirmative resolution of both Houses (see s330(5)(b)).[234]

The Labour Government had planned to seek affirmative resolutions from both Houses in autumn 2005, with a view to implementing section 43 in January 2006.[235] However, in March 2006 Lord Goldsmith, then Attorney General, announced that the Government no longer planned to bring forward an order giving effect to section 43, but would instead bring forward fresh primary legislation regarding fraud trials by jury.[236] The *Fraud (Trials Without a Jury) Bill* was brought forward in November 2006.[237] It completed its Commons stages but was blocked by the House of Lords at its Second Reading.[238]

Following the 2010 general election, the Government said that it would "protect historic freedoms through the defence of trial by jury".[239] **Clause 99** of the Bill would repeal section 43 of the 2003 Act.

11 Removal of restrictions on times for marriage and civil partnership

11.1 Background

Section 4 of the *Marriage Act 1949* provides that marriages may normally be solemnized between 8am and 6pm. There are some exceptions to this general rule: the time restriction does not apply to marriages of the terminally ill and to Jewish and Quaker marriages. Section 17(2) of the *Civil Partnership Act 2004* (as amended) imposes a similar time restriction for civil partnerships.

It is an offence to solemnize a marriage or to officiate at the signing of a civil partnership schedule outside the permitted hours.

---

234 Taylor, Wasik and Leng, *Blackstone's Guide to the Criminal Justice Act 2003*, 2004, p54
235 HL Deb 21 June 2005 cWS69 and HL Deb 27 October 2005 ccWS76-77
236 HL Deb 14 March 2006 c1128
237 See Library Research Paper 06/57 *The Fraud (Trials Without a Jury) Bill 2006-07* for background
238 HL Deb 20 March 2007 cc1146-1204
239 Cabinet Office, *The Coalition: our programme for government*, May 2010, p11

The Labour Government proposed that couples would be given a greater choice over the place and time of their marriage, as part of a more general reform of civil registration. Regulation of marriages was to be based on the celebrant rather than the building in which it takes place and it was intended that the couple would agree the time and place of their marriage with the celebrant.[240] However, these proposals were not implemented. Library Standard Note SN/HA/2842 *Marriage venues* includes further information.

Marriages in the Church of England and the Church in Wales must also, generally, take place between 8am and 6pm.[241]

11.2 The Bill's provisions

Clause 100 of the Bill would remove the time restrictions for marriage or civil partnership and the associated offences in England and Wales. This would mean, effectively, that either could take place at any time of the day or night (subject to there being someone available to officiate).

The amendment would not apply to Church of England marriages; an amendment to the canon law would be required, in addition, to effect this change. The process can take some years to complete. A press report quoted a Church of England spokesperson as saying that the church had no plans to alter the hours during which marriage ceremonies were conducted.[242]

---

[240] CM5355, *Civil Registration: Vital Change – Birth, Marriage and Death Registration in the 21st Century*, January 2002, p21

[241] *Canons of the Church of England,* sixth edition, 2000, B35; the Church in Wales website

[242] "Moonlight marriages get official blessing as night-time ban is lifted", *Independent,* 12 February 2011

Appendix 1: DNA Profile Retention Periods

Occurrence	Current System (E&W)	Crime & Security Act 2010 – E&W	Scottish System	Proposed changes under the Bill
ADULT – Conviction – All Crimes	Indefinite	Indefinite	Indefinite	Indefinite
ADULT – Non Conviction – Serious Crime	Indefinite*	6 Years	3 Years + possible 2-year extension(s) by Court	3 Years + possible single 2-Year extension by Court
ADULT – Non Conviction – Minor Crime	Indefinite*	6 Years	None	None†
UNDER 18s – Conviction – Serious Crime	Indefinite	Indefinite	Indefinite	Indefinite
UNDER 18s – Conviction – Minor Crime	Indefinite	1st Conviction – 5 years; 2nd – Indefinite	Indefinite	1st Conviction – 5 Years (plus length of any custodial sentence); 2nd Conviction – indefinite
UNDER 18s – Non Conviction – Serious Crime	Indefinite*	3 Years	3 Years + possible 2-year extension(s) by Court	3 Years + possible single 2-Year extension by Court
UNDER 18s – Non Conviction – Minor Crime	Indefinite*	3 Years	None	None†
Terrorist Suspects	Indefinite*	6 Years plus renewable 2-year period(s) on national security grounds	Not covered (reserved matters)	3 Years plus renewable 2 year period(s) on national security grounds
Biological DNA samples	Indefinite*	Within six months of sample being taken	As per destruction of profiles	Within six months of sample being taken

* Destruction of DNA profiles and biological samples is available under 'exceptional circumstances'. This requires an application to the Chief Constable of the relevant police force; removal from the database is then at his/her discretion in accordance with guidelines issued by the Association of Chief Police Officers.

† In all cases, a speculative search of the DNA and fingerprint databases may be conducted before destruction.

Source: *Protection of Freedoms Bill – Explanatory Notes*, Annex B