These notes refer to the Protection of Freedoms Act 2012 (c.9) which received Royal Assent on 1 May 2012

PROTECTION OF FREEDOMS ACT 2012

EXPLANATORY NOTES

INTRODUCTION

1. These Explanatory Notes relate to the Protection of Freedoms Act 2012 which received Royal Assent on 1 May 2012. They have been prepared by the Home Office in order to assist the reader in understanding the Act. They do not form part of the Act and have not been endorsed by Parliament.

2. The Notes need to be read in conjunction with the Act. They are not, and are not meant to be, a comprehensive description of the Act. So where a section or part of a section does not seem to require any explanation or comment, none is given.

3. A glossary of abbreviations and terms used in these Notes is contained in Annex A.

SUMMARY

4. The Act consists of seven Parts.

5. Chapter 1 of Part 1 makes provision in respect of the retention and destruction of fingerprints, footwear impressions and DNA samples and profiles taken in the course of a criminal investigation. In particular, it replaces the existing framework, set out in Part 5 of the Police and Criminal Evidence Act 1984 ("PACE"), whereby fingerprints and DNA profiles taken from a person arrested for, charged with or convicted of a recordable offence may be retained indefinitely. Under the new scheme provided for in this Chapter, the fingerprints and DNA profiles taken from persons arrested for or charged with a minor offence will be destroyed following either a decision not to charge or following acquittal. In the case of persons charged with, but not convicted of, a serious offence, fingerprints and DNA profiles may be retained for three years, with a single two-year extension available on application by a chief officer of police to a District Judge (Magistrates' Courts). The police will also be able to seek permission from the new independent Commissioner for the Retention and Use of Biometric Material to retain material for the same period (three plus two years) in cases where a person has been arrested for a qualifying offence but not charged. In addition, provision is made for the retention of fingerprints and DNA profiles in the case of persons convicted of an offence or given a fixed penalty notice and for extended retention on national security grounds.

6. Chapter 2 of Part 1 imposes a requirement on schools and further education colleges to obtain the consent of parents of children under 18 years of age attending the school or college, before the school or college can process a child's biometric information.

7. Chapter 1 of Part 2 makes provision for the further regulation of Closed Circuit Television ("CCTV"), Automatic Number Plate Recognition ("ANPR") and other surveillance camera technology operated by the police and local authorities. The provisions will require the Secretary of State to publish a code of practice in respect of the development and use of surveillance camera systems and provide for the appointment of a Surveillance Camera Commissioner to monitor the operation of the code.

8. Chapter 2 of Part 2 amends the Regulation of Investigatory Powers Act 2000 ("RIPA") so as to require local authorities to obtain judicial approval for the use of any one of the three covert investigatory techniques available to them under the Act, namely the acquisition and disclosure of communications data, and the use of directed surveillance and covert human intelligence sources ("CHIS").

9. Chapter 1 of Part 3 makes provision in respect of powers to enter land or other premises. The provisions enable a Minister of the Crown (or the Welsh Ministers), by order, to repeal unnecessary powers of entry, to add safeguards in respect of the exercise of such powers, or to replace such powers with new powers subject to additional safeguards. Each Cabinet Minister is placed under a duty to review existing powers of entry with a view to considering whether to exercise any of the aforementioned order-making powers. Provision is also made for the exercise of powers of entry to be subject to the provisions of a code of practice.

10. Chapter 2 of Part 3 makes provision in respect of parking enforcement. It makes it a criminal offence to immobilise a vehicle, move a vehicle or restrict the movement of a vehicle without lawful authority. Further provision is made to extend the power to make regulations for the police and others to remove vehicles that are illegally, dangerously or obstructively parked. Provision is also made so that the keeper (or in some circumstances the hirer) of a vehicle can be held liable for unpaid parking charges where the identity of the driver is not known.

11. Part 4 makes provision in respect of counter-terrorism powers. Sections 57 and 58 reduce the maximum period of pre-charge detention for terrorist suspects from 28 to 14 days whilst introducing a power for the Secretary of State to increase the limit to 28 days for a period of three months in circumstances where Parliament is dissolved or in the period before the first Queen's Speech of the new Parliament. Sections 59 to 63 relate to stop and search powers. They confer a power on a constable to search a vehicle if he or she reasonably suspects that a vehicle is being used for the purposes of terrorism; replace the powers to stop and search persons and vehicles without reasonable suspicion in sections 44 to 47 of the Terrorism Act 2000 ("the 2000 Act") with a power that is exercisable in more restricted circumstances; and similarly restrict the operation of the power to search persons and vehicles for munitions and transmitters without reasonable suspicion in Schedule 3 to the Justice and Security (Northern Ireland) Act 2007.

12. Chapter 1 of Part 5 amends the Safeguarding of Vulnerable Groups Act 2006 ("SVGA") which provides the framework for the vetting and barring scheme operated by the Independent Safeguarding Authority ("ISA") in England and Wales. The amendments, in particular, repeal the provisions of the SVGA which provide for the monitoring by the Secretary of State of persons engaging in regulated activity. This Chapter also provides for broadly similar changes to the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 ("SVGO") which provides the framework for the vetting and barring scheme in Northern Ireland.

13. Chapter 2 of Part 5 makes amendments to Part 5 of the Police Act 1997 ("the 1997 Act") which sets out the framework for the operation of the Criminal Records Bureau ("CRB") and the disclosure of criminal convictions and other relevant information in certificates issued by the CRB to support the assessment of a person's suitability for employment and other roles.

14. Chapter 3 of Part 5 establishes a new organisation, to be known as the Disclosure and Barring Service ("DBS"), which will replace and combine the functions of the ISA and the CRB.

15. Chapter 4 of Part 5 provides for a person to apply to the Secretary of State for a conviction or caution for an offence under section 12 or 13 of the Sexual Offences Act 1956 ("the 1956 Act"), and certain associated offences, involving consensual gay sex with another person aged 16 or over, to become a disregarded conviction or caution. This Chapter further provides for such disregarded convictions and cautions to be

deleted from the Police National Computer ("PNC") and other police records so that they no longer show up on criminal record checks.

16. Part 6 makes amendments to the Freedom of Information Act 2000 ("FOIA") and the Data Protection Act 1998 ("DPA"). The changes are fourfold. First, they amend the FOIA to make provision for the re-use of datasets by public authorities subject to that Act. Second, they amend the definition of a publicly owned company for the purposes of the FOIA so that it includes companies owned by two or more public authorities. Third, they extend to Northern Ireland amendments made to the FOIA by the Constitutional Reform and Governance Act 2010. Finally, they amend the FOIA and DPA to revise the arrangements in respect of the appointment and tenure of the office of the Information Commissioner and to make changes to the role of the Secretary of State in relation to the exercise of certain functions by the Information Commissioner.

17. Part 7 makes two principal changes to existing criminal offences on human trafficking. First, it expands the existing trafficking offences, currently set out in sections 57 to 59 of the Sexual Offences Act 2003 and in section 4 of the Asylum and Immigration (Treatment of Claimants etc.) Act 2004, which make it an offence to traffick a person into, within, or out of the United Kingdom for the purposes of exploitation. Part 7 will, in addition, make it an offence for a UK national to traffick a person for sexual exploitation or for the purpose of labour or other exploitation regardless of where in the world the trafficking occurs or is intended to occur; and regardless of where the facilitation or arrangement of the trafficking takes place. Secondly, Part 7 amends the 2004 Act so that it is an offence where the trafficking of a person for the purpose of labour or other exploitation takes place wholly within the United Kingdom.

18. Part 7 introduces into the Protection from Harassment Act 1997 two new offences of stalking (a summary only offence) and stalking involving fear of violence or serious alarm or distress (an either way offence). It also introduces a power of entry in relation to the summary only offence of stalking that would confer on the police a power, subject to the authorisation of a magistrate, to enter and search premises if there are reasonable grounds for believing that there is material on the premises which is likely to be of substantial value to the investigation of the offence.

19. Part 7 also contains two repeals of enactments. It repeals section 43 of the Criminal Justice Act 2003 ("the 2003 Act"), which makes provision for certain fraud trials to be conducted without a jury, and removes the restrictions on the times when a marriage or civil partnership can take place. This Part also contains consequential amendments and repeals, makes provision for transitional arrangements, determines the extent of the provisions in the Act and provides for commencement.

BACKGROUND

20. The Coalition's Programme for Government[1], launched by the Prime Minister and Deputy Prime Minister on 20 May 2010, included a commitment to introduce a 'Freedom' Bill. What is now the Protection of Freedoms Act contributes to the implementation of 12 other specific commitments in the Programme for Government.

Part 1: Regulation of biometric data

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

21. The Programme for Government (section 3: civil liberties) states that the Government "*will adopt the protections of the Scottish model for the DNA database*".

22. The existing framework for the taking, retention and destruction of fingerprints, footwear impressions, DNA samples and the profiles derived from such samples is set out in Part 5 of Police and Criminal Evidence Act 1984 ("PACE"). The amendments

1 http://webarchive.nationalarchives.gov.uk/20100526084809/http://programmeforgovernment.hmg.gov.uk

to PACE made by the Criminal Justice and Public Order Act 1994 ("the 1994 Act") enabled DNA samples to be taken from anyone charged with, reported for summons, cautioned or convicted of a recordable offence; and allowed profiles obtained from such samples to be retained and speculatively searched against other profiles obtained from victims or scenes of crime. A recordable offence is defined in section 118 of PACE. In practice, all offences which are punishable with imprisonment are recordable offences, as are around 60 other non-imprisonable offences that are specified in regulations made under section 27 of PACE. If the person was acquitted, samples and profiles were required to be destroyed. The passage of the 1994 Act led to the creation, in April 1995, of the National DNA Database in England and Wales.

23. The Criminal Justice and Police Act 2001 further amended PACE so as to remove the obligation to destroy a DNA sample or profile when a suspect was not prosecuted for or was acquitted of the offence with which he or she was charged. The power to take and retain DNA samples and profiles was further widened by the Criminal Justice Act 2003 ("the 2003 Act") which enabled a DNA sample to be taken from any person arrested for a recordable offence and detained in a police station, whether or not they are subsequently charged. Any such sample, and the profile derived from it, could be retained indefinitely.

24. In December 2008, in the case of *S and Marper v United Kingdom* [2008] ECHR 1581[2] the European Court of Human Rights ("ECtHR") ruled that the provisions in PACE (and the equivalent legislation in Northern Ireland), permitting the 'blanket and indiscriminate' retention of DNA from unconvicted individuals violated Article 8 (right to privacy) of the European Convention on Human Rights ("ECHR"). In response to this judgment, the then Government brought forward provisions in what are now sections 14 to 23 of the Crime and Security Act 2010 ("the 2010 Act") which, amongst other things, allowed for the retention of fingerprints and DNA profiles of persons arrested for, but not convicted of, any recordable offence for six years. Sections 14 to 18, 20 and 21 of the 2010 Act established a separate approach to the retention of DNA profiles and fingerprints by the police for national security purposes and made provisions for the extended retention of DNA and fingerprints on national security grounds. These provisions of the 2010 Act have not been brought into force and Part 1 of Schedule 10 to this Act repeals them.

25. The equivalent legislation in Scotland is contained in sections 18 to 20 of the Criminal Procedure (Scotland) Act 1995 (as amended). A table comparing the retention rules in respect of fingerprints and DNA samples and profiles as they are now, as they would have been under the provisions of the 2010 Act, as they currently operate in Scotland and as they would be under the provisions of this Act is at Annex B.

Chapter 2 of Part 1: Protection of biometric information of children in schools etc.

26. The Programme for Government (section 3: civil liberties) states that the Government "*will outlaw the finger-printing of children at school without parental permission*".

27. A number of schools in England and Wales currently use automated fingerprint recognition systems for a variety of purposes including controlling access to school buildings, monitoring attendance, recording the borrowing of library books and cashless catering. Iris, face and palm vein recognition systems are also in use or have been trialled. The processing of biometric information is subject to the provisions of the Data Protection Act 1998 ("DPA"), but whilst the DPA requires the data subject to be notified about the processing of his or her personal data and in most cases, to consent to such processing, there is no requirement, in the case of a person aged under 18 years, for consent also to be obtained from the data subject's parents. In August 2008 the Information Commissioner issued a statement on the use of biometric technologies

2 http://www.bailii.org/eu/cases/ECHR/2008/1581.html

in schools[3]. Guidance has also been issued, in July 2007, by the British Educational Communications and Technology Agency[4].

Part 2: Regulation of surveillance

Chapter 1: Regulation of CCTV and other surveillance camera technology

28. The Programme for Government (section 3: civil liberties) states that the Government "*will further regulate CCTV*".

29. CCTV systems (including ANPR systems) are not currently subject to any bespoke regulatory arrangements. However, the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the DPA and the Information Commissioner's Office ("ICO") has issued guidance to CCTV operators on compliance with their legal obligations under the DPA[5]. In addition, the covert use of CCTV systems is subject to the provisions of the Regulation of Investigatory Powers Act ("RIPA") and the Code of Practice on 'Covert Surveillance and Property Interference' issued under section 71 of that Act (see in particular paragraphs 2.27 to 2.28)[6]**.** On 15 December 2009, the previous Government announced the appointment of an interim CCTV Regulator (Hansard, House of Commons, columns 113WS-114WS).

Chapter 2 of Part 2: Safeguards for certain surveillance under RIPA

30. The Programme for Government (section 3: communities and local government) states that the Government "*will ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime*".

31. RIPA was designed to regulate the use of investigatory powers and to satisfy the requirements of the ECHR on its incorporation into UK law by the Human Rights Act 1998. RIPA regulates the use of a number of covert investigatory techniques, not all of which are available to local authorities. The three types of technique available to local authorities are: the acquisition and disclosure of communications data (such as telephone billing information or subscriber details); directed surveillance (covert surveillance of individuals in public places); and covert human intelligence sources ("CHIS") (such as the deployment of undercover officers). Local authorities sometimes need to use covert techniques in support of their statutory functions. They, not the police, are responsible for enforcing the law in areas such as: environmental crime; consumer scams; loan sharks; taxi cab regulation; underage sales of knives, alcohol, solvents and tobacco; and the employment of minors. The communications data powers are primarily used by local authorities to target rogue traders (where a mobile phone number can be the only intelligence lead). Directed surveillance powers are used in benefit fraud cases and to tackle anti-social behaviour (in partnership with the police), while CHIS and directed surveillance techniques are used in test purchase operations to investigate the sale of tobacco, alcohol and other age-restricted products.

32. Chapter 2 of Part 1 of RIPA sets out the specified grounds for authorising the acquisition and disclosure of communications data and Part 2 specifies the grounds for which authorisations can be granted for carrying out directed surveillance and for the use of CHIS. At present, authorisations for the use of these techniques are granted internally by a member of staff in a local authority (who must be of at least Director, Head of Service, Service Manager or equivalent grade), and are not subject to any independent approval mechanism. The use of these covert techniques under RIPA is subject to codes of practice made by the Home Secretary. The Chief Surveillance Commissioner

---

3 http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf
4 [ARCHIVED CONTENT] Becta Schools - Leadership and management - Introduction - Guidance on the use of biometric systems in schools
5 http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx
6 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert

is responsible for overseeing local authorities' use of directed surveillance and CHIS, whilst the Interception of Communications Commissioner has similar responsibilities in respect of local authorities' use of their powers in respect of the acquisition and disclosure of communications data. The Investigatory Powers Tribunal, established under section 65 of RIPA, investigates complaints about anything that a complainant believes has taken place against them, their property or communications which would fall to be regulated under RIPA.

33. The review of counter-terrorism and security powers (see paragraph 38) considered the use of RIPA powers by local authorities following concerns that they have been using directed surveillance techniques in less serious investigations, for example, to tackle dog fouling or checking an individual resides in a school catchment area. The review concluded (see paragraph 13, page 27 of the report[7]), that the use of directed surveillance powers by local authorities should be subject to a seriousness threshold and that the use of all three techniques by local authorities should be subject to a Magistrate's approval mechanism. The seriousness threshold will restrict local authority use of directed surveillance to the investigation of offences which attract a maximum custodial sentence of six months or more or which involve underage sales of alcohol and tobacco. The threshold will be introduced, in parallel with the Protection of Freedoms Act, through an order made under section 30(3)(b) of RIPA; Chapter 2 of Part 2 gives effect to the Magistrate's approval mechanism (in Scotland approval will be granted by a sheriff's court).

Part 3: Protection of property from disproportionate enforcement action

Chapter 1: Powers of Entry

34. A power of entry is a right for a person (usually a state official of a specified description, for example, police officers, local authority trading standards officers, or the enforcement staff of a regulatory body) to enter into a private dwelling, business premises, land or vehicles (or a combination of these) for defined purposes (for example, to search for and seize evidence as part of an investigation, or to inspect the premises to ascertain whether regulatory requirements have been complied with). There are around 1300 separate powers of entry contained in both primary and secondary legislation[8]. A Home Office-led review of powers of entry, initiated by the previous Administration in October 2007, was on-going at the time of the 2010 general election; background information about that review is archived on the Home Office website[9].

Chapter 2 of Part 3: Vehicles left on land

35. The Programme for Government (section 30: transport) states that the Government "*will tackle rogue private sector wheel clampers*".

36. Under the provisions of the Private Security Industry Act 2001 ("the 2001 Act") persons engaged in parking control on private land by means of the immobilisation (wheel clamping), moving or otherwise restricting the movement of a vehicle are required to be licensed by the Security Industry Authority ("SIA"). Continued concerns about the practices adopted by vehicle immobilisation businesses led the previous Government to publish, in April 2009, a consultation on options for improving the regulation of the clamping industry, including a voluntary code of practice and compulsory membership of a business licensing scheme for all clamping companies. The Crime and Security Act 2010 ("the 2010 Act"), which received Royal Assent on 8 April 2010, contains provisions for the licensing of businesses that undertake vehicle

---

7 http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/review-findings-and-rec?view=Binary
8 http://www.homeoffice.gov.uk/publications/about-us/legislation/powers-entry/
9 http://tna.europarchive.org/20100419081706/http:/www.police.homeoffice.gov.uk/operational-policing/powers-pace-codes/powers-of-entry-review/index67d9.html?version=2

immobilisation activities (see sections 42 to 44 of and Schedule 1 to that Act). The provisions of the 2010 Act have not been commenced.

37. On 17 August 2010 the Government announced proposals to prohibit the wheel clamping of vehicles on private land[10]. The prohibition would take the place of the current licensing of individual operatives engaged in wheel clamping and of the prospective licensing of wheel clamping businesses.

Part 4: Counter-terrorism powers

38. The Programme for Government (section 3: civil liberties) states that the Government "*will introduce safeguards against the misuse of anti-terrorism legislation*".

39. The Home Secretary announced a review of counter-terrorism and security powers in an oral statement to Parliament on 13 July 2010 (Hansard, House of Commons, columns 797 to 809; the statement was repeated in the House of Lords at columns 644 to 652). The terms of reference of the review were published on 29 July 2010[11], these set out the six key counter-terrorism and security powers to be considered by the review, namely:

- Control orders (including alternatives);
- Section 44 stop and search powers and the use of terrorism legislation in relation to photography;
- The use of the RIPA by local authorities and access to communications data more generally;
- Extending the use of 'Deportation with Assurances' in a manner that is consistent with our legal and human rights obligations;
- Measures to deal with organisations that promote hatred or violence; and
- The detention of terrorist suspects before charge, including how we can reduce the period of detention below 28 days.

40. The Home Secretary reported the outcome of the review[12] on 26 January 2011 in a further oral statement to Parliament (Hansard, House of Commons, columns 306 to 326; the statement was repeated in the House of Lords at columns 965 to 978). Lord Macdonald of River Glaven, who provided independent oversight of the review, published a separate report of his findings[13]. Chapter 2 of Part 2 and Part 4 give effect to the review's conclusions in respect of the use of RIPA powers by local authorities, stop and search powers, and the maximum period of pre-charge detention for terrorist suspects.

41. Part 5 of the Terrorism Act 2000 ("the 2000 Act") contains 'counter-terrorist powers' including two police stop and search powers. Section 43 of the 2000 Act enables a constable to stop and search a person they reasonably suspect to be a terrorist to discover whether that person has in his or her possession anything that may constitute evidence that they are a terrorist (this power extends to stopping but not to searching a vehicle). Section 44 (together with the associated provisions in sections 45 to 47) of the 2000 Act enables a constable to stop and search any person or any vehicle within an authorised area for the purposes of searching for articles of a kind that could be used in connection for terrorism; this power does not require any grounds for suspicion that such articles will be found.

---

10 http://www.homeoffice.gov.uk/media-centre/press-releases/ban-on-wheel-clamping
11 http://www.homeoffice.gov.uk/publications/counter-terrorism/ct-terms-of-ref/counter-terrorism-terms-of-ref?view=Html
12 http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/review-findings-and-rec?view=Binary
13 http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/report-by-lord-mcdonald?view=Binary

42. Following a challenge by two individuals stopped and searched under the section 44 powers in 2003, the ECtHR held on 12 January 2010, in the case of *Gillan and Quinton v UK (Application no. 4158/05)*, that the stop and search powers in section 44 violated Article 8 of the ECHR because they were insufficiently circumscribed and therefore not 'in accordance with the law'. This judgment became final on 28 June 2010 when the UK's request for the case to be referred to the Grand Chamber of the ECtHR was refused.

43. On 8 July 2010, the Home Secretary made a statement in the House of Commons (Hansard, House of Commons, columns 540 to 548; the statement was repeated in the House of Lords at columns 378 to 386) setting out how the powers in section 44 were to operate pending the outcome of the review of counter-terrorism and security powers and subsequent enactment of replacement legislation. In particular, the Home Secretary indicated that terrorism-related stops and searches of individuals were to be conducted under section 43 of the 2000 Act on the basis of reasonable suspicion that the individual is a terrorist and that section 44 (no suspicion) was no longer to be used for the searching of individuals. The Home Office publishes annual statistics on the operation of police powers under the 2000 Act; statistics covering the quarterly period to September 2011 were published on 22 March 2012[14].

44. Section 41 of and Schedule 8 to the 2000 Act brought into effect legislation on pre-charge detention which allowed the police to detain a terrorist suspect for up to seven days without charge (the maximum period of pre-charge detention for non-terrorist cases is four days). This period was increased to 14 days by section 306 of the Criminal Justice Act 2003 ("the 2003 Act"). The Terrorism Bill introduced in the 2005-06 Session by the then Government included amendments to Schedule 8 to the 2000 Act to extend the maximum period of pre-charge detention from 14 to 90 days. An amendment to that Bill to set the maximum period of pre-charge detention at 28 days was agreed by the House of Commons at Report Stage of the Bill on 9 November 2005 (Hansard, columns 325 to 387).

45. Under what is now section 25 of the Terrorism Act 2006 the 28 day maximum period of pre-charge detention is subject to renewal by affirmative order for periods of up to a year at a time, failing which the maximum period reverts to 14 days. Successive twelve-month orders were made in 2007, 2008 and 2009. The Counter-Terrorism Bill introduced in the 2007-08 session included provisions to extend the maximum period of pre-charge detention to 42 days. The relevant sections were rejected by the House of Lords at Committee Stage of the Bill on 13 October 2008 (Hansard, column 491 to 545), therefore preserving the 28 day maximum put in place by the Terrorism Act 2006.

46. Following debates in both the House of Commons[15] and the House of Lords[16], a new order (SI 2010/645) was made on 25 July 2010 retaining the 28 day maximum for a further six months pending the outcome of the review of counter-terrorism and security powers. That order expired on 24 January 2011.

47. In her oral statement on 26 January 2011, the Home Secretary indicated that the Government would place in the Library of the House of Commons draft emergency legislation which would, if enacted, extend the maximum period of pre-charge detention to 28 days for a period of three months. The Government would bring forward such legislation if there were exceptional circumstances where this longer period may be required. Two versions of the draft Counter-Terrorism (Temporary Provisions) Bill were published on 11 February 2011 and are available at the Home Office website: Home Office. The draft Bills were subject to pre-legislative scrutiny by a Joint Committee of both Houses of Parliament which reported on 23 June 2011[17]. The

---

14 http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/counter-terrorism-statistics/hosb0412/hosb0412?view=Binary
15 House of Commons Hansard Debates for 14 July 2010 (pt 0003)
16 Lords Hansard text for 19 Jul 201019 July 2010 (pt 0001)
17 http://www.parliament.uk/business/committees/committees-a-z/joint-select/joint-committee-on-the-draft-detention-of-terrorist-suspects-temporary-extension-bills/news/report-publication/

Government responded to that Report on 3 October; this response was published as a Command Paper Cm 8220 on 14 November 2011[18].

Part 5: Safeguarding vulnerable groups, criminal records etc.

Chapters 1 to 3: Safeguarding of vulnerable groups and criminal records

48. The Programme for Government (section 14: families and children) said "*we will review the criminal records and vetting and barring regime and scale it back to common sense levels*".

49. The vetting and barring scheme was established in response to a recommendation made by Sir Michael (now Lord) Bichard in his June 2004 report following an inquiry into the information management and child protection procedures of Humberside Police and Cambridgeshire Constabulary[19]; the Bichard Inquiry was established in response to the conviction of Ian Huntley, a school caretaker, for the murders of Holly Wells and Jessica Chapman. The Inquiry Report recommended, amongst other things, that a registration scheme should be established for those wishing to work with children or vulnerable adults.

50. The Safeguarding Vulnerable Groups Act 2006 ("SVGA") and the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 ("SVGO") provided for such a scheme maintained by the Independent Safeguarding Authority ("ISA")[20]. Originally some 11 million people working with children or vulnerable adults would have been required to be monitored under the Scheme. In response to concerns about the scope of the Scheme, the then Government commissioned its Chief Adviser on the Safety of Children, Sir Roger Singleton, to conduct a review of the Scheme. Sir Roger Singleton's report[21] and the Government's response were published on 14 December 2009 (Hansard, House of Commons, column 50WS to 53WS).

51. The revised vetting and barring scheme, as recommended by Sir Roger Singleton, would have involved some 9.3 million individuals. On 15 June 2010 the Home Secretary announced that voluntary applications to be monitored under the Scheme, which was due to begin on 26 July 2010, would be suspended pending a further review and remodelling of the Scheme (Hansard, House of Commons, column 46WS to 47WS). The Home Secretary announced the terms of reference of the remodelling review on 2 October 2010 (Hansard, House of Commons, column 77WS to 78WS), as follows:

    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.

---

18 http://www.official-documents.gov.uk/document/cm82/8220/8220.pdf
19 http://www.bichardinquiry.org.uk/10663/report.pdf
20 The ISA was originally known as the Independent Barring Board; the change of name was made by section 81 of the Policing and Crime Act 2009.
21 'Drawing the Line' – A Report on the Government's Vetting and Barring Scheme, available at: https://www.education.gov.uk/publications/eOrderingDownload/DCSF-01122-2009.pdf

52. The report of the remodelling review was published on 11 February 2011[22]. Amongst other things, the report recommended that the requirement on those working with children and vulnerable adults to be monitored under the Scheme should be dropped and that the functions of the ISA and the Criminal Records Bureau ("CRB") should be brought together into a single new organisation. Chapters 1 and 3 of Part 5 give effect to the report's recommendations.

53. Part 5 of the Police Act 1997 ("the 1997 Act") makes provision for the Secretary of State to issue certificates to applicants containing details of their criminal records and other relevant information. In England and Wales this function is exercised on behalf of the Secretary of State by the CRB, an executive agency of the Home Office. These certificates are generally used to enable employers and prospective employers or voluntary organisations to assess a person's suitability for employment or voluntary work, particularly where this would give the person access to children or vulnerable adults. The CRB has operated since March 2002.

54. Part 5 of the 1997 Act provides for three types of certificate:

- A criminal conviction certificate (known as a 'basic certificate') which includes details of any convictions not "spent" under the terms of the Rehabilitation of Offenders Act 1974. Basic certificates are not yet available from the CRB;
- A criminal record certificate (known as a 'standard certificate') which includes details of all convictions and cautions held on police records (principally, the Police National Computer ("PNC")), whether those convictions and cautions are spent or unspent; and
- An enhanced criminal record certificate (known as an 'enhanced certificate') which includes the same information as would appear on a standard certificate together with any other relevant, non-conviction information contained in police records held locally and, in appropriate cases, barred list information held by the ISA.

55. Mrs Sunita Mason was appointed by the previous Administration in September 2009 as the Government's Independent Adviser for Criminality Information Management and was commissioned to undertake a review of the arrangements for retaining and disclosing records held on the PNC. Mrs Mason's report[23] was published on 18 March 2010 alongside the Government response set out in a Written Ministerial Statement (Hansard, House of Commons, column 73WS).

56. On 22 October 2010, the Home Secretary announced a further review, again by Mrs Mason, of the criminal records regime (Hansard, House of Commons, columns 77WS to 78WS). The review was to be undertaken in two phases. The questions to be addressed by Mrs Mason in the first phase were:

- Could the balance between civil liberties and public protection be improved by scaling back the employment vetting systems which involve the CRB?
- Where Ministers decide such systems are necessary, could they be made more proportionate and less burdensome?
- Should police intelligence form part of CRB disclosures?

57. Mrs Mason's report on phase one of the review was published on 11 February 2011[24]. Amongst the recommendations made in the report were:

- children under 16 should not be eligible for criminal record checks (recommendation 1);

---

22 http://www.homeoffice.gov.uk/publications/legislation/protection-freedoms-bill/
23 'A Balanced Approach: Safeguarding the public through the fair and proportionate use of accurate criminal record information' available at http://library.npia.police.uk/docs/homeoffice/balanced-approach-criminal-record-information.pdf
24 http://www.homeoffice.gov.uk/publications/legislation/protection-freedoms-bill/

- criminal records checks should be portable between positions within the same employment sector (recommendation 2);
- the CRB to introduce an online system to allow employers to check if updated information is held about an applicant (recommendation 3);
- a new CRB procedure to be developed so that the criminal record certificate is issued directly to the individual applicant who will be responsible for its disclosure to potential employers and/or voluntary bodies (recommendation 4);
- the introduction of a package of measures to improve the disclosure of police information to employers (recommendation 6). This included -
  - the test used by chief officers to make disclosure decisions under section 113B(4) of the 1997 Act to be amended from 'might be relevant' to 'reasonably believes to be relevant' (recommendation 6a);
  - the development of a statutory code of practice for the police to use when deciding what information should be disclosed (recommendation 6b);
  - the current 'additional information' provisions under section 113B(5) of the 1997 Act to be abolished so that the police use alternative methods to disclose this information outside of the criminal record disclosure process (recommendation 6e);
  - to make effective use of the Police National Database so that decision making by chief officers about the relevancy of information in relation to enhanced criminal record certificates can be centralised, regardless of from which police force the information originated (recommendation 6f).
- the CRB to develop an open and transparent representations process for individuals to challenge inaccurate or inappropriate disclosures and that the disclosure of police information is overseen by an independent expert (recommendation 7).

58. Chapter 2 of Part 5 gives effect to these recommendations.

Chapter 4 of Part 5: Disregarding certain convictions for buggery etc.

59. The Programme for Government (section 20: justice) said "*we will change the law so that historical convictions for consensual gay sex with over -16s will be treated as spent and will not show up on criminal records checks*".

60. The offences that criminalised consensual sex between men over the age of consent in England and Wales were section 12 of the Sexual Offences Act 1956 ("the 1956 Act") for the offence of buggery and section 13 of the 1956 Act for the offence of gross indecency between men. Consensual sex in private between two men over the age of 21 was decriminalised by section 1 of the Sexual Offences Act 1967; in 1994 the age of consent was lowered to the age of 18 years (by sections 143 and 145 of the Criminal Justice and Public Order Act 1994); in 2000 it was lowered again to 16 years (by section 1 of the Sexual Offences (Amendment) Act 2000). Such convictions, however, continue to be recorded in police records, principally on the names database held on the Police National Computer ("PNC"), and will appear on a standard or enhanced criminal records certificate issued by the CRB. It is estimated that there are some 12,000 such convictions recorded on the PNC.

Part 6: Freedom of information and data protection

61. The Programme for Government (section 3: civil liberties and section 16: government transparency) states that the Government will: "*extend the scope of the Freedom of Information Act to provide greater transparency*"; "*create a new 'right to data' so that government-held datasets can be requested and used by the public, and then published*

on a regular basis"; and "*ensure that all data published by public bodies is published in an open and standardised format, so that it can be used easily and with minimal cost by third parties*".

62. The Office of Information Commissioner was created in January 2005 on the coming into force of the Freedom of Information Act 2000 ("FOIA"). The Information Commissioner's role absorbed that of the Data Protection Registrar, first established by section 3 of the Data Protection Act 1984 ("the 1984 Act"); the 1984 Act was repealed by the Data Protection Act 1998 ("DPA"), section 6 of which provided for the continuation of the Data Protection Registrar's office under the new name of "the office of the Data Protection Commissioner". The Information Commissioner is the independent regulator for information rights in the UK and has responsibility for the oversight of both the DPA and FOIA. The Commissioner also has responsibility for the Environmental Information Regulations 2004 (SI 2004/3391), which implement Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information, and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), which implement Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

63. The Information Commissioner's Office ("ICO") is an executive Non-Departmental Public Body sponsored by the Ministry of Justice. The Commissioner is appointed as a corporation sole by Her Majesty by letters patent on the recommendation of the Prime Minister, who is advised by the Secretary of State for Justice following a selection process undertaken by the Ministry of Justice and validated by the Office of the Commissioner for Public Appointments. The current Commissioner, Christopher Graham, took up his five year appointment in June 2009.

64. The provisions in the DPA and FOIA cover the Commissioner's appointment, remuneration and funding, appointment of staff and officers of the ICO, accountability and the Commissioner's functions. Although the Commissioner operates independently in the exercise of his or her statutory functions, some issues require the approval of the Secretary of State such as funding, the level of certain fees charged by the ICO and the issue of codes of practice.

65. The FOIA confers a general right of access to information held by over 100,000 public authorities in the UK. Once a person makes an application, the public authority has 20 working days to respond to the request or notify the individual making the request why the information required is exempt. The Act recognises that there will be valid reasons why some kinds of information may be withheld, such as if its release would prejudice national security or legitimate commercial confidentiality. Public authorities can also refuse a freedom of information request if collating the information would incur disproportionate costs.

66. All public authorities, and companies wholly owned by a single public authority, have obligations under the FOIA and the Information Commissioner is responsible for issuing guidance on set procedures for responding to requests. The Commissioner also receives complaints about public authorities' conduct of their responsibilities. After investigation the Information Commissioner makes a final assessment as to whether or not the relevant public authority has complied with the Act. Enforcement action may be taken against public authorities that repeatedly fail to meet their responsibilities under the Act.

67. The FOIA makes no express provision in respect of datasets. The Government's proposals to make available Government data were set out in a letter, dated 31 May 2010, from the Prime Minister to Departments[25]. Government datasets are available at: www.data.gov.uk.

25 Letter to Government departments on opening up data | Number10.gov.uk

68. The Government's proposals for extending the scope of the FOIA were announced on 7 January 2011[26].

Part 7: Miscellaneous and general

Trafficking people for exploitation

69. On 29 March 2010, the European Commission tabled its proposal for a directive on trafficking in human beings; the EU agreed a finalised text in March 2011 which was adopted on 5 April 2011 (Directive 2011/36/EU of the European Parliament and of the Council on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decisions 2002/629/JHA)[27]. The UK applied to opt in to the Directive in July 2011 and in October 2011, received confirmation from the European Commission that its application had been accepted. The UK is already compliant with most of the requirements of the Directive; however, there are two aspects which require primary legislation in order to comply. Government is now working on implementing the Directive to ensure compliance by the April 2013 deadline.

70. The offences of harassment and putting people in fear of violence in the Protection from Harassment Act 1997 came into force on 16 June of that year. That Act criminalises harassment and the more serious offence of pursuing a course of conduct putting people in fear of violence. On 14 November 2011 the Home Office launched a consultation to ask for views on how to protect victims of stalking more effectively and whether or not a change in the law was required; there were 156 responses to the consultation, which closed on 5 February 2012.

Repeal of provisions for conducting certain fraud cases without jury

71. The Programme for Government (section 3: civil liberties) states that the Government "*will protect historic freedoms through the defence of trial by jury*".

72. Section 43 of the Criminal Justice Act 2003 ("the 2003 Act") makes provision for the prosecution to apply for a serious or complex fraud trial to proceed in the absence of a jury. The judge may order the case to be conducted without a jury if he or she is satisfied that the length or complexity (or both) of the case is likely to make the trial so burdensome upon the jury that the interests of justice require serious consideration to be given to conducting the trial without a jury.

73. Section 43 has not been implemented. By virtue of section 330(5)(b) of the 2003 Act, an order bringing section 43 into force is subject to the affirmative resolution procedure. A draft commencement order designed to bring section 43 of the 2003 Act into force was considered in standing committee in the House of Commons in November 2005. The order was then due to be debated in the House of Lords but the then Government withdrew the motion to approve it. Subsequently, in November 2006, the Government introduced the Fraud (Trials without a Jury) Bill which sought to repeal the requirement for an affirmative resolution. That Bill was defeated at Second Reading in the House of Lords on 20 March 2007 (Hansard, column 1146-1204).

TERRITORIAL EXTENT

74. The majority of the Act's provisions extend to England and Wales only, but certain provisions also extend to Scotland or Northern Ireland or both. In relation to Scotland, the Act addresses non-devolved matters only; in relation to Wales and Northern Ireland the Act addresses both devolved and non-devolved matters.

75. The following provisions in the Act which extend to Scotland relate to reserved matters:

---

26 Opening up public bodies to public scrutiny - Ministry of Justice
27 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:EN:PDF

- The retention of fingerprints and DNA profiles subject to the Terrorism Act 2000 ("the 2000 Act") or retained for national security purposes (sections 19 to 22 and Parts 1 and 3 to 5 of Schedule 1);
- The requirement for local authorities to obtain judicial approval for the application and use of communications data under Regulation of Investigatory Powers ("RIPA") (Chapter 2 of Part 2);
- The provisions in respect of certain powers of entry insofar as such powers relate to reserved matters (Chapter 1 of Part 3);
- The provisions in respect of the maximum periods of pre-charge detention for terrorist suspects (sections 57 and 58);
- The changes to terrorism stop and search powers in sections 59 to 62 and Schedule 5;
- The amendments to the Freedom of Information Act 2000 ("FOIA") and the Data Protection Act 1998 ("DPA") (section 86 and Part 6); and
- The power of the Treasury to make provision in respect of taxation in connection with the transfer of property, rights or liabilities of the ISA and the CRB to the Disclosure and Barring Service (section 91).

76. This Act does not contain any provisions falling within the terms of the Sewel Convention.

77. In relation to Wales, the provisions of the Act do not relate to devolved matters or confer functions on the Welsh Ministers except for the following:

- The requirement to obtain parental consent before processing a child's biometric information in schools and colleges (Chapter 2 of Part 1);
- Powers of entry - Chapter 1 of Part 3 confers powers on the Welsh Ministers to make orders repealing, adding safeguards to or rewriting powers of entry and to make a code of practice in relation to powers of entry (and associated powers) in so far as such powers of entry relate to transferred matters;
- The provision to make the vehicle keeper responsible in certain circumstances for unpaid parking related charges (section 56 and Schedule 4); and
- The amendments to the Safeguarding Vulnerable Groups Act 2006 and the establishment of the Disclosure and Barring Service (Chapters 1 and 3 of Part 5).

78. The National Assembly for Wales agreed a legislative consent motion in respect of these provisions on 15 March 2011 (see Official Report at The Record).

79. On 5 May 2011, the Assembly Act provisions of the Government of Wales Act 2006 came into force. Amongst other things, these provisions extended the legislative competence of the National Assembly of Wales to include matters in respect of access to information held by the National Assembly for Wales, the Assembly Commission, the Welsh Assembly Government or Welsh public authorities. Accordingly, to the extent that the provisions in Part 6 of the Act amending the FOIA relate to such matters, those provisions now also relate to devolved matters. The National Assembly for Wales agreed a legislative consent motion in respect of these provisions on 31 January 2012.

80. The provisions of the Act relating to the following excepted or reserved matters also extend to Northern Ireland:

- The retention of fingerprints and DNA profiles subject to the 2000 Act or the Counter-Terrorism Act 2008 ("the 2008 Act"), or retained for national security

purposes and for the purposes connected with the International Criminal Court (sections 19 to 22 and Parts 1 to 4, 6 and 7 of Schedule 1);

- The requirement for local authorities to obtain judicial approval for the application and use of covert surveillance powers under RIPA (Chapter 2 of Part 2);
- The provisions relating to powers of entry insofar as they relate to excepted or reserved matters (Chapter 1 of Part 3);
- The provisions in respect of the maximum periods of pre-charge detention for terrorist suspects (sections 57 and 58);
- Changes to the terrorism stop and search powers, including amendments to the stop and search powers in Schedule 3 to the Justice and Security (Northern Ireland) Act 2007 (Part 4);
- The amendments to the DPA (section 86 and Part 6); and
- The power of the Treasury to make provision in respect of taxation in connection with the transfer of property, rights or liabilities of the ISA and the CRB to the Disclosure and Barring Service (section 91).

81. In addition, the following provisions of the Act relating to transferred matters will also extend to Northern Ireland:

- The amendments to the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 ("SVGO") (section 78 and Schedule 7) and the Disclosure and Barring Service (Chapter 3 of Part 5 and Schedule 8); and
- The amendments to the FOIA (sections 102, 103, 104, 105(5) and 107(3) and (4)).

82. As these provisions relate to transferred matters they require the consent of the Northern Ireland Assembly. The Northern Ireland Assembly agreed a legislative consent motion in respect of the amendments to the SVGO on 21 March 2011 (see Official Report at: The Assembly - Official Report Monday 21 March 2011). A further legislative consent motion was agreed by the Assembly on 27 June 2011[28] in relation to the Disclosure and Barring Service provisions in Chapter 3 of Part 5 and Schedule 8. On 26 September 2011[29], the Assembly also agreed a legislative consent motion in relation to the amendments to the FOIA made by Part 6.

THE ACT

Commentary on Sections

Part 1: Regulation of biometric data

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

Section 1: Destruction of fingerprints and DNA profiles

83. Section 1 inserts new section 63D into the Police and Criminal Evidence Act 1984 ("PACE") which sets out the basic rules governing the destruction of fingerprints and DNA profiles (collectively referred to as 'section 63D material') taken from a person under the powers in Part 5 of PACE or given voluntarily in connection with the investigation of an offence. New section 63D(2) requires the destruction of section 63D material if it appears to the responsible chief officer of police that the material was taken unlawfully, or that the material was taken from a person following an unlawful arrest or where the arrest was as a result of mistaken identity. Any other section 63D material must be destroyed as soon as reasonably practicable, subject to the operation of the

28 Northern Ireland Assembly minutes of proceedings 27.06.11
29 The Assembly - Official Report Monday 26 September 2011

provisions in new sections 63E to 63O and 63U of PACE detailed below. It is a general feature of new sections 63D to 63O that material must be destroyed unless one or more of those sections applies to that material, in which case the section which delivers the longest retention period will determine the period of retention. New section 63U(3), as inserted by section 17, provides that section 63D material need not be destroyed where it may be fall to be disclosed under the Criminal Procedure and Investigations Act 1996 or its attendant Code of Practice.

84. New section 63D(5) of PACE enables a person's section 63D material, which would otherwise fall to be destroyed, to be retained for a short period until a speculative search of the relevant databases has been carried out. The fingerprints and DNA profile of an arrested person will be searched against the national fingerprint and DNA databases respectively to ascertain whether they match any other fingerprints or DNA profile on those databases. Where such a match occurs, it may serve to confirm the person's identity, indicate that he or she had previously been arrested under a different name, or indicate that the person may be linked to a crime scene from which fingerprints or a DNA sample had been taken.

Section 2: Material retained pending investigation or proceedings

85. Section 2 inserts new section 63E into PACE, which enables material taken from a person in connection with the investigation of an offence to be retained until the conclusion of the investigation by the police or, where legal proceedings are instituted against the person, until the conclusion of those proceedings (for example, the point that charges are dropped or at the outcome of a trial).

Section 3: Persons arrested for or charged with a qualifying offence

86. Section 3 inserts new section 63F into PACE which provides for the further retention of material taken from persons (both adults and juveniles) arrested for or charged with a qualifying offence, but not subsequently convicted. The concept of a qualifying offence is used to distinguish between serious and less serious offences for the purposes of the retention regime. A list of qualifying offences is contained in section 65A(2) of PACE (as inserted by section 7 of the Crime and Security Act 2010 ("the 2010 Act")); the list broadly covers serious violent, sexual and terrorist offences. Where a person who is arrested for, but not convicted of, a qualifying offence has previously been convicted of a recordable offence, that is not an 'excluded offence', his or her section 63D material may be retained indefinitely (new section 63F(2)). A recordable offence is defined in section 118 of PACE. In practice, all offences which are punishable with imprisonment are recordable offences, as are around 60 other non-imprisonable offences which are specified in regulations made under section 27 of PACE. An excluded offence for these purposes is defined in new section 63F(11) of PACE (inserted by the section) as a conviction for a minor (that is, non-qualifying) offence, committed when the person was under the age of 18, for which a sentence of less than five years imprisonment (or equivalent) was imposed.

87. Where a person who is charged with, but not convicted of, a qualifying offence has no previous convictions, his or her section 63D material may be retained for three years (new sections 63F(3), (4) and (6)). Where a person with no previous convictions is arrested for a qualifying offence, but is not subsequently charged or convicted, his or her section 63D material may be retained for three years only if a successful application is made under new section 63G to the independent Commissioner for the Retention and Use of Biometric Material appointed under section 20(1) of the Act (new section 63F(5)).

88. The standard three-year retention period (whether following being charged with a qualifying offence, or arrested for such an offence and a successful application to the Commissioner) may be extended on a case by case basis with the approval of a District Judge (Magistrates' Courts). In any particular case, the police may apply during the last

three months of the three-year period to a District Judge (Magistrates' Court) for an order extending the retention period by an additional two years (new section 63F(7), (8) and (9)). The retention period cannot be extended beyond five years in total under this process. The police may appeal to the Crown Court against a refusal by a District Judge (Magistrates' Court) to grant such an order and the person from whom the material was taken may similarly appeal to the Crown Court against the making of such an order (new section 63F(10)). Separate arrangements (see new section 63M, inserted by section 9) apply in cases where the retention period is to be extended on national security grounds.

89. New section 63G sets out the procedure for the police to apply to the independent Commissioner for the Retention and Use of Biometric Material to retain section 63D material from a person with no previous convictions who has been arrested for a qualifying offence, but not subsequently charged or convicted. Applications may be made on the basis that either the victim of the alleged offence is vulnerable (which is defined as being under the age of 18, a vulnerable adult or in a close personal relationship with the arrested person) or, in other cases, where the police consider that retention is necessary for the prevention or detection of crime (new section 63G(2) and (3)). Notice of such an application must be given to the person to whom the section 63D material relates (new section 63G(6) to (8)) and that person may make representations to the Commissioner in respect of an application (new section 63G(5)).

Section 4: Persons arrested for or charged with a minor offence

90. Section 4 inserts new section 63H into PACE. Where a person is arrested for or charged with a minor offence (that is, a recordable offence which is not a qualifying offence) and is not subsequently convicted, their section 63D material must be destroyed, unless they have previously been convicted of a recordable offence that is not an 'excluded offence' (new section 63H(2)) in which case the material can be retained indefinitely. An excluded offence has the same meaning as in section 3 (new section 63H(3)).

Section 5: Persons convicted of a recordable offence

91. Section 5 inserts new section 63I into PACE, which governs the retention period applicable where a person has been convicted of a recordable offence. Where an adult is convicted of a recordable offence, his or her section 63D material may be retained indefinitely (as now). Where a person under the age of 18 is convicted of a recordable offence, if that offence is a qualifying offence his or her fingerprints and DNA profile may also be retained indefinitely (as now). The retention period in respect of a person under 18 convicted of his or her first minor offence is governed by new section 63K of PACE (see section 7).

Section 6: Persons convicted of an offence outside England and Wales

92. Section 6 inserts new section 63J into PACE. The existing sections 61 to 63 of PACE (as amended by section 3 of the 2010 Act) include provisions to take fingerprints and DNA samples from persons convicted of a qualifying offence outside England and Wales. New section 63J provides that section 63D material obtained under those provisions may be retained indefinitely.

Section 7: Persons under 18 convicted of first minor offence

93. Section 7, which inserts new section 63K into PACE, makes provision for the retention of section 63D material taken from persons convicted of a first minor offence, committed when they were under the age of 18. In such cases, the retention period is to be determined by the length and nature of the sentence for that minor offence. Where a custodial sentence of five or more years is imposed, the person's section 63D material may be retained indefinitely (new section 63K(3)). Where a custodial sentence of less than five years is imposed, the person's section 63D material may be retained for the duration of the sentence (both the period spent in custody and the period of the sentence

served in the community) plus a further five years (new section 63K(2)). Where a young person is given a non-custodial sentence on conviction for his or her first minor offence, his or her section 63D material may be retained for five years from the date the material was taken (new section 63K(4)). Any subsequent conviction for the recordable offence, whether before or after they turn 18, will enable the section 63D material to be retained indefinitely (new section 63J(5)).

Section 8: Persons given a penalty notice

94. Section 8 inserts new section 63L into PACE, which provides that, where a person is given a penalty notice under section 2 of the Criminal Justice and Police Act 2001, his or her section 63D material may be retained for two years from the date the material was taken (new section 63L(2)). Where a person opts to be tried for the offence for which the penalty notice was issued, that notice will be disregarded and the rules set out in the previous sections will apply (new section 63L(1)(a)).

Section 9: Material retained for purposes of national security

95. Section 9 inserts new section 63M of PACE which makes provision for the retention of material for the purposes of national security. Where a person's section 63D material would otherwise fall to be destroyed, it may be retained for up to two years where the responsible chief officer of police determines that it is necessary to retain it for the purposes of national security (a 'national security determination'). A responsible chief officer may renew a national security determination in respect of the same material, thus further extending the retention period by up to two years at a time. See section 20 (paragraphs 129 to 133) which set out the functions of the Commissioner for the Retention and Use of Biometric Material in respect of national security determinations.

Section 10: Material given voluntarily

96. Section 10 inserts new section 63N into PACE, which provides for section 63D material that has been given voluntarily to be destroyed as soon as it has fulfilled the purpose for which it was taken, unless the individual is previously or subsequently convicted of a recordable offence, in which case it can be retained indefinitely (new section 63N(3)).

Section 11: Material retained with consent

97. Section 11 inserts new section 63O into PACE. New section 63O provides that a person's section 63D material, which would otherwise fall to be destroyed, may be retained for as long as that person consents in writing to its retention. This provision applies both to material taken in accordance with the powers in Part 5 of PACE and to material given voluntarily. A person may withdraw his or her consent at any time (new section 63O(3)).

Section 12: Material obtained for one purpose and used for another

98. This section inserts new section 63P into PACE. Under new section 63P, where a person arrested for one offence is subsequently arrested for, charged with or convicted of a second unrelated offence, the retention of that person's section 63D material will be governed by the rules applicable to the second offence.

Section 13: Destruction of copies

99. Section 13 inserts new section 63Q into PACE which provides that all copies of fingerprints and DNA profiles held by the police must be destroyed when the obligation to destroy material set out in section 1 applies. This would also cover material held on behalf of the police by those providing services under contract, such as on the national databases or in forensic science laboratories.

Section 14: Destruction of samples

100. Section 14 inserts new section 63R into PACE, which provides for the immediate destruction of samples if it appears to the responsible chief officer of police that the material was taken unlawfully, or where the material was taken from a person following an unlawful arrest or where the arrest was as a result of mistaken identity (that is, in the same circumstances as section 63D material (see new section 63D(2), as inserted by section 1). In addition, DNA samples must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample (including the carrying out of the necessary quality and integrity checks) and, in any event, within six months of the taking of the sample. Any other sample, such as a blood or urine sample taken to test for alcohol or drugs, must similarly be destroyed within six months of it having been taken (new section 63R(5)).

101. New sections 63R(6) to (12) of PACE provide that samples may be retained for a longer period than six months in certain limited circumstances. Those circumstances are where it appears to the responsible chief officer of police that, in relation to a serious offence, it is necessary to ensure that key evidence (in the form of DNA samples) remains available for disclosure to the defendant or to respond to an evidential challenge by the defendant. In such cases, the decision to extend the permissible retention period would fall to a District Judge (Magistrates' Court) following an *ex parte* application made by the chief officer. If the application was approved, the district judge would authorise retention of the material for 12 months, which may be extended (on one or more occasions) following a further (*inter partes*) application by the responsible chief officer. Any material retained in this way would only be available for use in that case and the police would be under a duty to notify the person whose sample was to be retained, including any application for a subsequent order to retain and the outcome.

102. New section 63R(13) of PACE enables a person's DNA or other sample, which would otherwise fall to be destroyed, to be retained until a DNA profile has been derived from the sample and a speculative search of the relevant database has been carried out (that is, in the same circumstances as section 63D material (see new section 63D(5)).

Section 15: Destruction of impressions of footwear

103. Section 15 inserts new section 63S into PACE, which governs the retention and destruction of impressions of footwear. Where a footwear impression has been taken under section 61A of PACE or otherwise is obtained in connection with the investigation of an offence, it must be destroyed unless it is necessary to retain it for any of the purposes set out in new section 63S(3).

Section 16: Use of retained material

104. Section 16 inserts new section 63T into PACE which restricts the use to which fingerprints, DNA and other samples, DNA profiles and footwear impressions may be put. Such material may only be used for the purposes set out in new section 63T(1). New section 63T(2) provides that material which should otherwise have been destroyed in accordance with new sections 63D, 63R and 63S of PACE must not be used against the person to whom the material relates or for the purposes of the investigation of any offence; any evidence arising from the impermissible use of such material would therefore be likely to be ruled inadmissible in criminal proceedings.

Section 17: Exclusions for certain regimes

105. This section inserts new section 63U into PACE, which excludes from the PACE retention regime set out above those persons whose biometric data is held under the Terrorism Act 2000 Act ("the 2000 Act"), the International Criminal Court Act 2001 and the Terrorism Prevention and Investigation Measures Act 2011, as well as those whose fingerprints are held under immigration powers. A broadly equivalent retention

regime for terrorist suspects is provided for in Schedule 8 to the 2000 Act, as amended by Part 1 of Schedule 1 to this Act.

106. New section 63U(5) provides that section 63D material need not be destroyed where it may fall to be disclosed under the Criminal Procedure and Investigations Act 1996 or its attendant Code of Practice. Where section 63D material is retained in order to comply with that Act, it will be removed from the National DNA Database and held only in hard copy on the police case file, where it will be available for use only in connection with that particular case.

107. New section 63U(6) provides that section 63D material need not be destroyed where it relates to the biometric material of another person other than the one from whom it was taken. This would apply, for example, to material transferred in the course of a physical encounter, such as an assault, where one party's DNA or saliva is recovered from the other party.

Section 18: Interpretation and minor amendments of PACE

108. *Subsection (2)* adds definitions of a "DNA profile", "DNA sample", "responsible chief officer of police", "section 63D material" and "terrorist investigation" into the list of definitions in section 65(1) of PACE.

109. *Subsection (3)* inserts new subsections (2A) and (2B) into section 65 of PACE. New section 65(2A) ensures that destruction of a DNA sample under section 14 of the Act does not give the police grounds to take a fresh sample, while new section 65(2B) provides that, in new sections 63F, 63H, 63P and 63U, the definition of persons who are 'charged with an offence' includes (where Part 4 of the Criminal Justice Act 2003 is not in force) those who are informed that they will be reported to a Magistrates' Court for the issue of a summons to begin criminal proceedings.

110. *Subsection (4)* adds the offences of robbery and assault with intent to rob under section 8 of the Theft Act 1968 to the definition of qualifying offences in section 65A(2) of PACE.

111. *Subsection (5)* inserts new section 65B into PACE, which provides that, for the purpose of the rules set out in new sections 63D to 63U of PACE (as inserted by sections 1 to 17) governing the retention of fingerprints and DNA profiles, a person who has been given a caution (or, in the case of a person under 18, a warning or reprimand) is to be treated in the same way as a person who has been convicted of an offence. In addition, those individuals found not guilty by reason of insanity or otherwise to have committed the offence while under a disability will also be treated as having been convicted of an offence for the purpose of the retention rules as set out in those sections of PACE. New section 65B(2) provides that the retention rules in Part 5 of PACE, as amended, are to apply irrespective of the provisions of the Rehabilitation of Offences Act 1974 (under that Act certain offences are treated as being spent, and therefore to be disregarded for most purposes, after the expiry of specified rehabilitation periods). However, by virtue of new section 65B(3), a person is not to be regarded as having been convicted of or cautioned for an offence under section 12 (buggery) or 13 (gross indecency between men) of the Sexual Offences Act 1956 ("the 1956 Act") (and similar offences) if that conviction or caution is disregarded under the provisions in Chapter 4 of Part 5 of this Act. Accordingly, if a person was arrested for an offence and that person had no previous conviction save for a disregarded conviction, his fingerprints and DNA profile taken following the arrest could not be retained indefinitely as would be the case if the previous conviction or caution for an offence under section 12 or 13 of the 1956 Act had not been disregarded.

Section 19: Amendments of regimes other than PACE

112. Section 19 gives effect to Schedule 1.

Schedule 1: Amendments of regimes other than PACE

Part 1: Material subject to the Terrorism Act 2000

113. Paragraph 14 of Schedule 8 to the Terrorism Act 2000 ("the 2000 Act") as originally enacted provides for the retention of fingerprints and samples (and DNA profiles derived from samples) taken from persons detained under section 41 of or Schedule 7 to the 2000 Act (that is persons arrested as a suspected terrorist or persons detained under the ports and border control provisions in Schedule 7) without reference to a retention period. Paragraph 14 of Schedule 8 also sets out the purposes for which these fingerprints, samples and profiles may be used.

114. Paragraph 14 of Schedule 8 to the 2000 Act is repealed by Part 1 of Schedule 1 to this Act. *Paragraph 1(4)* inserts new paragraphs 20A to 20I into Schedule 8 of the 2000 Act, which make provision for a destruction and retention regime broadly equivalent to that set out in new sections 63D to 63T of PACE. It is a general feature that material must be destroyed unless it is retained under a power conferred under new paragraphs 20B to 20E; except in the case of samples which must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample and in any event within six months of taking the sample (new paragraph 20G). New paragraphs 20(6) to 20(13) replicate the provisions in new sections 63R(6) to (12) of PACE (see paragraph 101 above) to provide that samples may be retained for a longer period than six months in certain circumstances. The time limits for retention depend on whether the person has previous convictions or one exempt conviction (that is, a conviction for a minor offence committed when they were under 18) and whether the person has been detained under section 41 (arrest on reasonable suspicion of being a terrorist) of, or under Schedule 7 (detention at ports and borders) to, the 2000 Act. Where, following detention under section 41 or Schedule 7, the person is convicted of a recordable offence in England and Wales or Northern Ireland or an offence punishable by imprisonment in Scotland (or where the person already has such a conviction in England and Wales or Northern Ireland, other than an exempt conviction), the material need not be destroyed and may be retained indefinitely.

115. As is the case in relation to section 63D material in PACE, where fingerprints or DNA profiles would otherwise need to be destroyed, if a chief officer of police (or chief constable in Northern Ireland) determines that it is necessary to retain that material for the purposes of national security, that material may be further retained for up to two years (new paragraph 20E). It is open to that chief officer to renew a national security determination in respect of the same material to further extend the retention period by up to two years at a time.

116. New paragraph 20F replicates the effect of the new provisions in new section 63Q of PACE in relation to the destruction of copies of fingerprints and DNA profiles. New paragraph 20H largely replicates the provisions as originally enacted in paragraph 14 of Schedule 8 to the 2000 Act (as prospectively amended by section 16 of the Counter-Terrorism Act 2008 ("the 2008 Act")) in relation to the uses to which retained material may be put; it may be used in the interests of national security, for the purposes of a terrorist investigation, for the investigation of crime or for identification-related purposes (*sub-paragraph (1)*). Where a responsible chief officer of police considers that a relevant search (that is, the checking of fingerprints or DNA profiles against other material held) is desirable, paragraph 20H(2) provides an express power to carry out such a search. Paragraph 20H(3) is also new, and provides that, once the new requirement to destroy material applies, the material cannot be used in evidence against the person to whom it relates or for the purposes of the investigation of any offence.

117. New paragraph 20I replicates the new section 63U(3) of PACE (see section 17) to provide that material taken from a person detained under section 41 of the 2000 Act need not be destroyed where it may fall to be disclosed under the Criminal Procedure and Investigations Act 1996 or its Code of Practice. Where material is retained in order

to comply with that Act, it will be removed from the relevant database and held only in hard copy on the police case file, where it will be available for use only in connection with that particular case.

118. *Paragraph 1(5)* to *(8)* makes further consequential amendments to Schedule 8 to the 2000 Act.

Part 2: Material subject to the International Criminal Court Act 2001

119. Fingerprints and samples may be taken from a person under Schedule 4 to the International Criminal Court Act 2001 if the International Criminal Court ("ICC") requests assistance in obtaining evidence of the identity of a person (who will usually be a person suspected of committing an "ICC crime" such as genocide or war crimes). Under new section 63U(3) of PACE, inserted by section 17 of this Act, the regime in Chapter 1 of Part 1 of this Act does not apply to such material. Part 2 of Schedule 1 instead substitutes a new paragraph 8 of Schedule 4 to the International Criminal Court Act 2001 to make provision for the retention and destruction of material taken under that Schedule, so that all material must be destroyed within six months of it being transferred to the ICC or, if later, as soon as it has fulfilled the purposes for which it was taken.

Part 3: National security material subject to section 18 of the Counter-Terrorism Act 2008

120. Part 3 inserts a new section 18 and new sections 18A to 18E into the 2008 Act (section 18 of the 2008 Act has not been brought into force). New section 18 makes provision for the destruction of national security material that is not subject to existing statutory restrictions.

121. New section 18 makes provision for the retention, by law enforcement authorities under the law of England and Wales and Northern Ireland, of fingerprints, DNA samples and profiles on national security grounds which has been obtained by or supplied to the authority in the way described in section 18(3) (mostly covertly acquired material and material supplied by overseas authorities) and which is not subject to "existing statutory restrictions", such as those set out in the Immigration Act 1971, PACE, the PACE (Northern Ireland) Order 1989, or in Schedule 8 to the 2000 Act. It is a general feature that material must be destroyed unless it is retained under a power conferred under new sections 18A and 18B; except in the case of samples which must be destroyed as soon as a DNA profile has been satisfactorily derived from the sample and in any event within six months of taking the sample.

122. New section 18A makes provision for limited retention of material taken from persons with no previous convictions. New section 18B provides for extended retention for the purposes of national security. Where fingerprints or DNA profiles would otherwise need to be destroyed (because of the expiry of a time limit set out in the new provisions), if the 'responsible officer' determines that it is necessary to retain that material for the purposes of national security, those fingerprints or DNA profiles may be further retained for up to two years. It is open to that chief officer to renew a national security determination in respect of the same material to further extend the retention period by up to two years at a time. 'Responsible officer' is defined in new section 18E.

123. New section 18C replicates the effect of the new provisions in new section 63Q of PACE (destruction of copies) and new paragraph 20F of Schedule 8 to the 2000 Act about the destruction of copies of fingerprints and DNA profiles that are held by a law enforcement agency. New section 18D makes provision about the purposes for which material may be used which are the same as those now included in new section 63T of PACE. It also includes (new section 18(2)) an express power for section 18 material to be checked against other material (held by law enforcement authorities or the Scottish Police Services Authority). New section 18D(3) provides that, once the new requirement to destroy material applies, the material cannot be used in evidence against

the person to whom it relates or for the purposes of the investigation of any offence. New section 18E provides definitions of terms used in new sections 18 to 18D.

Part 4: Material subject to the Terrorism Prevention and Investigation Measures Act 2011

124. *Paragraph 5* amends Schedule 6 to the Terrorism Prevention and Investigation Measures ("TPIM") Act 2011 which makes provision for the taking and retention of biometric material from a person subject to a TPIM notice. This paragraph makes similar provision to new section 65B(3) of PACE (see section 18), namely that for the purpose of the rules set down in Schedule 6 to the TPIM Act governing the retention of fingerprints and DNA profiles, a person is not to be regarded as having been convicted of or cautioned for an offence under section 12 (buggery) or 13 (gross indecency between men) of the Sexual Offences Act 1956 (and similar offences) if that conviction or caution is disregarded under the provisions of Chapter 4 of Part 5 of the Act.

Part 5: Material subject to the Criminal Procedure (Scotland) Act 1995

125. *Paragraph 6(3)* inserts new section 18G into the Criminal Procedure (Scotland) Act 1995 This provides that where relevant physical data, samples or information derived from samples taken under the powers mentioned in that new section would otherwise need to be destroyed because of the expiry of a time limit set out in the new provisions, if the 'relevant chief constable' determines that it is necessary to retain that material for the purposes of national security, those fingerprints or DNA profiles may be further retained for up to two years. The relevant chief constable may make further determinations to retain the material, which again have effect for a maximum of two years. 'Relevant chief constable' is defined in new section 18G(6) and *paragraph 6(2)* makes a consequential amendment to the Criminal Procedure (Scotland) Act.

Part 6: Material subject to the Police and Criminal Evidence (Northern Ireland) Order 1989

126. This Part makes provision in respect of Northern Ireland equivalent to that in section 9 (material retained for the purposes of national security) in respect of England and Wales.

Part 7: Corresponding Northern Ireland provision for excepted or reserved matters etc.

127. Part 7 confers two order-making powers on the Secretary of State to amend the Police and Criminal Evidence (Northern Ireland) Order 1989 in respect of the retention and destruction of fingerprints and DNA for excepted or reserved purposes, that is, where retention is in the interests of national security or for the purposes of a terrorist investigation, and in respect of a transferred matter where that matter is ancillary to a reserved or excepted matter. The Police and Criminal Evidence (Northern Ireland) Order 1989 makes provision for the taking, retention and destruction of fingerprints and DNA by police in Northern Ireland for transferred purposes and closely reflects the provisions in Part 5 of PACE which operates in England and Wales. The order making powers conferred on the Secretary of State by *paragraph 8(2)* and *(3)* are required as the Northern Ireland Assembly is expected to legislate in the near future, following public consultation, in relation to the taking and retention of fingerprints and DNA for transferred purposes (in response to the ECtHR judgment in the case of *S and Marper v UK* [2008] ECHR 1581). It is only when this legislation is enacted that the Secretary of State can make certain further provision in relation to excepted and reserved matters. By virtue of *paragraph 8(6)* and *(7)*, an order made under this paragraph is subject to the affirmative resolution procedure if it amends or repeals primary legislation but is otherwise subject to the negative resolution procedure.

Section 20: Appointment and functions of Commissioner

128. *Subsection (1)* places a duty on the Secretary of State to appoint a Commissioner for the Retention and Use of Biometric Material (the Commissioner). *Subsection (10)* makes provision for the terms of the Commissioner's appointment and for the payment of allowances to the Commissioner and of his or her expenses. *Subsection (11)* enables the Secretary of State to provide staff, accommodation, equipment and other facilities to support the work of the Commissioner.

129. *Subsection (2)* confers on the Commissioner the function of keeping under review determinations made by chief officers of police and others that the fingerprints and DNA profiles of a person are required to be retained for national security purposes, and the use to which fingerprints and DNA profiles so retained are being put.

130. To enable the Commissioner to discharge this function, *subsection (3)* requires persons making national security determinations to notify the Commissioner in writing of the making of a determination, including a statement of the reasons why it was made, and to provide such other documents or information as the Commissioner may require in the exercise of his or her functions.

131. *Subsections (4)* and *(5)* enable the Commissioner, having reviewed a national security determination, to order the destruction of the fingerprints and DNA profile held pursuant to it where he or she is satisfied that a determination should not have been made. There is no appeal against such a ruling by the Commissioner save by way of judicial review. The Commissioner may not order the destruction of material that could otherwise be retained pursuant to any other statutory provision, for example under the provisions in new section 63F(5) and (9) of PACE (as inserted by section 3).

132. *Subsections (6)* to *(8)* confer on the Commissioner a general function of keeping under review the retention and use, by the police and others, of fingerprints and DNA profiles not subject to a national security determination, whether taken under PACE, the 2000 Act, the 2008 Act or the TPIM Act 2011.

133. *Subsection (9)* provides that the Commissioner also has the function of determining (in response to applications by the police) whether the fingerprints and DNA profiles of persons arrested for, but not charged with, a qualifying offence may be retained pursuant to the provisions in new section 63G of PACE (as inserted by section 3 of this Act).

Section 21: Reports by Commissioner

134. *Subsections (1)* and *(2)* require that the Commissioner make an annual report to the Secretary of State and enables the Commissioner to make such other reports on any matter relating to the Commissioner's functions. The Secretary of State may also, at any time, commission a report from the Commissioner on any matter relating to the retention and use of biometric material by law enforcement authorities for national security purposes (*subsection (3)*). The Secretary of State is required to lay any report from the Commissioner before Parliament, but before doing so he or she may exclude from publication any part of the report which would, in his or her opinion, be contrary to the public interest or prejudicial to national security (*subsections (4)* and *(5)*).

Section 22: Guidance on making national security determinations

135. *Subsection (1)* places a duty on the Secretary of State to issue guidance as to the making or renewing of national security determinations. The draft of such guidance, and any revisions to it, must be laid before each House of Parliament which must approve an order giving effect to the guidance, or revised guidance, before it can come into force (*subsections (5)* and *(6)*). Chief officers of police and others who may make national security determinations are required to have regard to such guidance (*subsection (2)*).

Section 23: Inclusion of DNA profiles on National DNA Database

136. Section 23 inserts a new section 63AA into PACE which places on a statutory footing the existing National DNA Database. The new section requires DNA profiles taken under PACE or in connection with an investigation to be recorded on the relevant database. The National DNA Database is maintained and operated by the National Police Improvement Agency on behalf of the police.

Section 24: National DNA Database Strategy Board

137. Section 24 inserts new section 63AB into PACE, which provides for the Secretary of State to make arrangements for a National DNA Database Strategy Board. Such a Board already exists, and reports to the Home Secretary, providing strategic oversight of the application of powers under PACE for taking and using DNA. The principal members of the Board are the Association of Chief Police Officers, the Association of Police Authorities (in future, a representative of Police and Crime Commissioners following their election towards the end of 2012) and the Home Office, but there is also an independent element to the Board from non-police bodies such as the Information Commissioner and the National DNA Database Ethics Group. This section puts the Board on a statutory footing and requires the Secretary of State to lay the Board's governance rules and annual reports before Parliament (new section 63AB(8) and (9)).

138. New section 63AB(2) requires the Board to issue guidance to chief officers on the circumstances in which DNA samples and profiles should be removed immediately from the National DNA Database. Chief officers will be required to act in accordance with the Board's guidance (new section 63AB(3)). Following consultation with the Commissioner for the Retention and Use of Biometric Material the Board will also have the power to issue guidance to the police on the making of applications under new section 63G (inserted by section 3) to retain material from those arrested for, but charged with, a qualifying offence (new section 63AB(4) and (5)).

Section 25: Material taken before commencement

139. Section 25 requires the Secretary of State to make an order (subject to the negative resolution procedure) prescribing the manner, timing and other procedures in respect of destroying relevant biometric material already in existence at the point this legislation comes into force. This will enable the Secretary of State to ensure that the retention and destruction regime set out in Chapter 1 of Part 1 of the Act is applied to existing material, while recognising that this exercise may take some time to complete; for example, there are just over one million profiles of unconvicted persons on the National DNA Database.

Chapter 2 of Part 1: Protection of biometric information of children in schools etc.

Section 26: Requirement for consent before processing biometric information

140. *Subsections (1)* to *(3)* provide that proprietors of schools or the governing bodies of colleges must notify the parents of a child that they intend to process the child's biometric information and that parents may object, in writing, to the processing. If no parent objects to the processing, the written consent of only one parent will be required. A child means any person under the age of 18 (see section 28(1)). Consent under this provision is only required if the information is to be used for the purposes of an automated biometric recognition system (defined in section 28(4)), such as a finger-print recognition system.

141. *Subsection (5)* provides that proprietors of schools and the governing bodies of colleges must not process, or continue to process, a child's biometric data if that child objects to its processing, irrespective of the child's age, maturity or ability to understand. This is the case even if consent has been given by a parent to the information being processed.

142. *Subsection (7)* requires schools and colleges to provide a child with a reasonable alternative to an automated biometric system where the child objects to the processing of his or her biometric information, or where any parent objects in writing to such processing. Such alternatives must allow the child to access any facility (for example, library facilities) that they would have had access to if using the biometric system, and to be subject to any monitoring or control (for example, monitoring of attendance) that they would have been subject to if using the biometric system.

Section 27: Exceptions and further provision about consent

143. *Subsection (1)* sets out certain exceptions to the requirement that consent be obtained from a parent including circumstances where a parent cannot be found, a parent lacks the mental capacity to consent and where the child's welfare requires that a parent is not contacted.

144. *Subsection (2)* provides that a notification from the school or college to parents about the processing of biometric information must be made in writing and that any objections from parents must also be in writing. Where consent is given verbally, the school cannot process the child's biometric information; any withdrawal of consent must also be in writing.

145. *Subsection (3)* provides that consent given by a parent to a school or college to process their child's biometric data can be withdrawn at any time. *Subsection (4)* provides that consent must be given, and (if withdrawn), withdrawn, in writing. Once consent is withdrawn, the proprietors of the school or college must stop processing the child's biometric data. The Data Protection Act 1998 will, in such circumstances, require that any personal data held by the school or college for the purposes of a biometric identification system must be destroyed; the school or college should do so as soon as practicable.

Section 28: Interpretation: Chapter 2

146. This section defines various terms used in Chapter 2 of Part 1.

147. *Subsection (2)* defines 'biometric information' as information about a person's physical or behavioural characteristics or features from which he or she can be identified, and which have been obtained or recorded so that it can be used for the purposes of an automated biometric recognition system. *Subsection (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. *Subsection (4)* defines a biometric recognition system as a system which operates automatically and processes biometric information in order to recognise or identify an individual.

148. *Subsections (5)* to *(8)* define who is a 'parent' for the purpose of Chapter 2. The definition is such that, under section 26, consent must be obtained from a child's mother, father or any other individual who has parental responsibility for the child. *Subsections (6)* to (8) apply where it has not been possible to obtain consent from any of these individuals; in such circumstances consent is to be sought from the child's carers unless the child has been placed with the carer by a local authority or a voluntary organisation, in which case, parental consent must be obtained from the local authority or, as the case may be, the voluntary organisation.

Part 2: Regulation of surveillance

Chapter 1: Regulation of CCTV and other surveillance camera technology

Section 29: Code of practice for surveillance camera systems

149. *Subsection (1)* requires the Secretary of State to prepare a code of practice in relation to surveillance camera systems. The term 'surveillance camera systems' is defined in *subsection (6)*, which includes Closed Circuit Television ("CCTV") and Automatic Number Plate Recognition ("ANPR") systems. *Subsection (2)* stipulates that the code must include guidance in relation to the development or use of such systems, or the use and processing of images derived from them. The latter could include, for example, what images are retained; how they are stored and for how long; and to what uses they might subsequently be put.

150. *Subsection (3)* lists more detailed issues that may be included in the code. These include advice about factors to consider when deciding whether the use of such equipment is appropriate (*subsection (3)(a)*); standards for equipment and operators (*subsection (3)(c),(f)* and *(g)*); and the provision of information to the public about aspects of such systems, including complaints procedures (*subsection (3)(e)* and *(i)*).

151. *Subsection (4)* provides that the code need not provide guidance in relation to every type of surveillance camera system. This is intended primarily to avoid a requirement to provide comprehensive guidance in relation to niche or emerging technologies not yet likely to have widespread application. It further provides that the extent of any guidance provided need not be identical in respect of each type of system, or may be suitably tailored to the type and usage of the system in question.

152. *Subsection (5)* requires the Secretary of State when preparing a code of practice to consult certain specified bodies and office holders, namely: the representative bodies of persons required to have regard to the code (as provided for in section 33(1)); the Association of Chief Police Officers; the Information Commissioner (responsible for the oversight of the Data Protection Act 1998; the Chief Surveillance Commissioner (appointed under Part 3 of the Police Act 1997 and responsible for oversight of the conduct of covert surveillance and covert human intelligence sources under that Act and the Regulation of Investigatory Powers Act 2000; the Surveillance Camera Commissioner (see section 34); and the Welsh Ministers. Other persons may be added to this list at the discretion of the Secretary of State.

Section 30: Issuing of the code

153. This section sets out the parliamentary procedure for approving the first surveillance camera code made under the preceding section. *Subsection (1)* requires the Secretary of State to lay the proposed code before Parliament together with a draft order bringing the code into force. Such an order is subject to the affirmative resolution procedure (*subsection (2)*). If the draft order bringing into force the first code of practice is not approved the Secretary of State is required to prepare a revised code; the draft order bringing such a revised code into force is again subject to the affirmative procedure (*subsection (4)*).

154. *Subsection (7)* disapplies the hybridity procedure should such procedure apply to the order made under this section. Some statutory instruments which need to be approved by both Houses are ruled to be hybrid instruments because they affect some members of a group (be it individuals or bodies) more than others in the same group. Hybrid instruments are subject to a special procedure which gives those who are especially affected by them the opportunity to present their arguments against the statutory instrument to the Hybrid Instruments Committee and then, possibly, to a Select Committee charged with reporting on its merits. The hybrid instrument procedure is unique to the House of Lords and the process must be completed before the instrument can be approved by both Houses.

Section 31: Alteration or replacement of the code

155. This section places a duty on the Secretary of State to keep the surveillance camera code of practice under review; the Secretary of State may, in the light of such a review, amend the existing code or substitute a new code (*subsection (1)*). *Subsection (2)* requires that in making any alteration to the code or when introducing a new code the Secretary of State must again consult the persons listed in section 29(5). *Subsections (3)* to *(9)* makes provision relating to the issuing of a replacement or amended code. In particular, either House of Parliament has 40 days (excluding any period during which Parliament is not sitting for more than four days) in which to pass a resolution refusing to approve the code. If such a resolution is passed then the Secretary of State may prepare another code of practice or amended code of practice for resubmission. Where no resolution is passed, the replacement or amended code will come into force at the end of the 40-day period.

Section 32: Publication of code

156. This section requires the Secretary of State to publish the surveillance camera code of practice once approved under section 30, and any subsequent revisions to that code or any replacement code.

Section 33: Effect of code

157. *Subsection (1)* provides that certain specified bodies or organisations (referred to as a "relevant authority") must have regard to the code if they operate or intend to operate any surveillance camera systems covered by the code. The bodies designated in the first instance as relevant authorities are set out in *subsection (5)*, namely local authorities, police and crime commissioners and chief officers of police.

158. *Subsection (5)(k)* provides that the Secretary of State may, by order (subject to the affirmative resolution procedure (*subsection (9)*)), designate other individuals or bodies, or descriptions thereof, as "relevant authorities" for the purposes of this section, thus requiring such designated bodies also to have regard to the code. Such an order may provide that a person designated as a relevant authority by virtue of such order is only required to have regard to the surveillance camera code of practice when discharging specified functions or acting in a specified capacity (*subsection (6)* and *(7)*). This is intended to provide for those instances where certain bodies have a dual role 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. Before making such an order the Secretary of State must consult the persons to be affected by it, or their representative body, together with other specified persons (*subsection (8)*). *Subsection (10)* disapplies the hybridity procedure should such procedure apply to an order made under subsection (5)(k).

159. *Subsection (2)* provides that a failure to adhere to any aspects of the code of practice would not, of itself, render a person liable to civil or criminal proceedings. However, the surveillance camera code is admissible in criminal or civil proceedings (*subsection (3)*) and a court or tribunal may take into account any failure of a relevant authority to comply with the duty to have regard to the code (*subsection (4)*).

Section 34: Commissioner in relation to code

160. *Subsection (1)* requires the Secretary of State to appoint a Surveillance Camera Commissioner. *Subsection (2)* sets out the Commissioner's responsibilities, namely promoting and encouraging compliance with the surveillance camera code of practice amongst users; reviewing how the code is working; and providing advice about the code (which may include, for example, advice to users of surveillance systems, members of the public, and Ministers as necessary). *Subsection (3)* makes provision for the terms of the Commissioner's appointment and for the payment of allowances to the Commissioner and of his or her expenses. *Subsection (4)* enables the Secretary of State

to provide staff, accommodation, equipment and other facilities to support the work of the Commissioner.

Section 35: Reports by Commissioner

161. Section 35 requires the Commissioner to send an annual report to the Secretary of State who must, in turn, lay the report before Parliament. The Commissioner must publish the report (*subsection (1)*).

Section 36: Interpretation: Chapter 1

162. Section 36 contains definitions of the terms "the Commissioner", "surveillance camera code" and "surveillance camera systems" as used in this Chapter.

Chapter 2 of Part 2: Safeguards for certain surveillance under RIPA

Section 37: Judicial approval for obtaining or disclosing communications data

163. Section 37 inserts new sections 23A and 23B into the Regulation of Investigatory Powers Act 2000 ("RIPA") which provide a procedure by which local authority authorisations or notices to obtain "communications data", or renewals of those authorisations or notices, can only come into effect if approved by a relevant judicial authority. In England and Wales, the judicial authority is a justice of the peace (Magistrates' Court), in Northern Ireland it is a district judge (magistrates' court) and in Scotland, a sheriff. The section also provides a mechanism by which the requirement for judicial approval may be applied to authorisations or notices granted by officials in other public authorities by order made by the Secretary of State.

164. Communications data is defined in section 21 of RIPA. In summary it is information such as telephone numbers dialled, times of calls, details of callers and receivers, and website addresses. In the case of postal items, communications data includes anything written on the outside of the item. Under Chapter 2 of Part 1 of RIPA, conduct consisting in the acquisition or disclosure of communications data is rendered lawful if it is authorised or carried out pursuant to an authorisation or notice granted or given in accordance with the provisions in sections 22 and 23 of RIPA.

165. Authorisations must not be granted or renewed, and notices must not be given or renewed, save by a person of a description designated by order under section 25(2) of RIPA. The designated person must not grant or renew an authorisation, or give or renew a notice, unless they believe that it is necessary to obtain the data on grounds specified in section 22 of RIPA, and that obtaining the data in question is proportionate to what is sought to be achieved by obtaining the data. By section 25(3), the Secretary of State may by order impose restrictions on the types of authorisations or notices that may be granted by individuals within specified public authorities, and on the circumstances in which, and the purposes for which, authorisations may be granted or notices given by those individuals. In the case of local authorities, such designated persons must be staff of at least Director, Head of Service or Service Manager grade or equivalent. These designated persons may not grant authorisations or notices save for the purpose of preventing or detecting crime or preventing disorder (see the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480)).

166. New section 23A(1) of RIPA provides that new section 23A applies where a "relevant person" has granted or renewed an authorisation, or given or renewed a notice under section 22 of RIPA. New section 23A(6) defines a "relevant person" for these purposes as either a designated person within a local authority in England, Wales or Scotland, or a designated person in Northern Ireland where the grant, renewal or authorisation relates to an excepted or reserved matter. A relevant person may also be any other person of a description prescribed by order of the Secretary of State. Such an order cannot make provision in relation to a matter that has been transferred to the competence of the Northern Ireland Assembly. An order made by the Secretary of State to prescribe

additional relevant persons to whom the judicial approval requirement will apply would be subject to the affirmative resolution procedure (new section 23A(7)). By this mechanism the requirement to obtain judicial approval for the use of the powers to obtain or disclose communications data will only initially apply to local authorities, but the Secretary of State will subsequently be able to extend the requirement to other public bodies able to exercise these powers.

167. New section 23A(2) provides that an authorisation or notice granted or renewed under the relevant provisions in section 22 of RIPA will not take effect until the "relevant judicial authority" has given its approval. The relevant judicial authority is defined in new section 23A(6).

168. New section 23A(3) sets out the test for the judicial approval of a local authority authorisation, or renewal of an authorisation, to obtain communications data. The relevant judicial authority must be satisfied that not only were there reasonable grounds for the designated person to believe that obtaining communications data was necessary and proportionate (subsection (3)(a)(i)), but that there also remain reasonable grounds for believing so (subsection (3)(b)). The judicial authority must also be satisfied that the "relevant conditions", which relate to the authorisation or notice, were met (subsection (3)(a)(ii)). New section 23A(4) sets out the same test for the judicial approval of the giving and renewal of notices to obtain communications data.

169. New section 23A(5) lists the relevant conditions that must be met if the relevant judicial authority is to approve the making or renewing of an authorisation or notice. For local authorities, in England, Wales and Scotland (and in Northern Ireland where the authorisation or notice is granted or given for the purpose relating to an excepted or reserved matter), these conditions are: (a) whether the person making the authorisation was of the correct office, rank or position and was accordingly a designated person within the meaning of Chapter 2 of Part 1 of RIPA; (b) whether the authorisation or notice was in breach of any other restrictions imposed by the Secretary of State by virtue of the power at section 25(3); and (c) whether the authorisation or notice satisfied any other conditions set out in an order (subject to the negative resolution procedure) made by the Secretary of State. In relation to conditions (a) and (b), the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) applies. For authorisations or notices granted or given by public authorities other than local authorities to which the judicial approval requirement may in the future be applied, the relevant conditions are those that will be set out in an order (subject to the negative resolution procedure) made by the Secretary of State. New section 23A(6) defines various terms used in new section 23A.

170. New section 23B sets out the procedure for obtaining judicial approval for an authorisation, or notice, to obtain communications data.

171. New section 23B(1) provides that the public authority to which the relevant person (authorising officer) belongs may apply for approval from the relevant judicial authority for an authorisation or a notice to obtain communications data. The relevant person is not required to apply in person; the same procedure applies to renewals.

172. New section 23B(2) provides that notice of such applications need not be given to either the subject of the authorisation or notice or to their legal representatives; this reflects the covert nature of the exercise of the investigatory powers under RIPA.

173. New section 23B(3) allows the relevant judicial authority on refusing an approval of an authorisation or a notice to quash that authorisation or notice.

Section 38: Judicial approval for directed surveillance and covert human intelligence sources

174. *Subsection (1)* inserts new sections 32A and 32B into RIPA which provide a procedure by which local authority authorisations in England, Wales and Northern Ireland for

the use of directed surveillance and the conduct and use of covert human intelligence sources ("CHIS") can only come into effect if approved by a relevant judicial authority. In England and Wales the judicial authority is a justice of the peace (Magistrates' Court). In Northern Ireland it is a district judge (magistrates' court). The requirements also apply to renewals of authorisations. The section further provides a mechanism by which the requirement for judicial approval may be applied to authorisations granted by officials in other public authorities by order made by the Secretary of State.

175. Directed surveillance is defined in section 26(2) of RIPA as covert surveillance otherwise than by way of an immediate response to events or circumstances for the purpose of a specific investigation which is likely to obtain private information and which is not intrusive surveillance (that is, it is not surveillance carried out in relation to anything taking place on residential premises or in any private vehicle). A CHIS is defined in section 26(8) of RIPA as a person who establishes or maintains a personal or other relationship with another for, amongst other things, the covert purpose of using such a relationship to obtain or disclose information to others.

176. Under Part 2 of RIPA, directed surveillance or the conduct and use of a CHIS is rendered lawful if it is authorised and carried out pursuant to an authorisation granted under section 28 of RIPA (for directed surveillance) or section 29 of RIPA (for CHIS). An authorisation may not be granted except by a person designated by order made under section 30(1) of RIPA. The designated person must not grant or renew the authorisation unless they believe that the conduct is necessary on grounds specified in section 28(3) or section 29(3) of RIPA, and that the conduct is proportionate to what is sought to be achieved by carrying it out. By section 30(3), the Secretary of State may by order impose restrictions on the types of authorisations that may be granted by individuals within specified public authorities, and on the circumstances in which and the purposes for which authorisations may be granted or renewed by those individuals. In the case of local authorities, such designated persons must be staff of at least Director, Head of Service or Service Manager grade or equivalent. These designated persons must not grant or renew the authorisations save for the purposes of preventing or detecting serious crime or preventing disorder (see the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Services) Order 2010 (SI 2010/521)).

177. New section 32A(1) provides that new section 32(A) applies where a "relevant person" has granted an authorisation under section 28 (authorisation of directed surveillance) or section 29 (authorisation of CHIS) of RIPA. New section 32A(7) defines a relevant person for these purposes as either a designated person in a local authority in England and Wales, or a designated person in Northern Ireland where the grant relates to an excepted or reserved matter. A relevant person may also be any other person of a description prescribed by order of the Secretary of State. Such an order cannot make provision in relation to a matter that has been transferred to the competence of the Northern Ireland Assembly. An order made by the Secretary of State to prescribe additional relevant persons to whom the judicial approval requirement will apply would be subject to the affirmative resolution procedure (new section 32A(8)). By this mechanism the requirement to obtain judicial approval for the use of the powers in respect of directed surveillance or CHIS will only initially apply to local authorities, but the Secretary of State will subsequently be able to extend the requirement to obtain judicial approval to other public bodies able to exercise these powers.

178. New section 32A(2) provides that an authorisation granted under the relevant provisions in section 28 or section 29 of RIPA will not take effect until the "relevant judicial authority" has given its approval. The relevant judicial authority for these purposes is defined in new section 32A(7).

179. New section 32A(3) sets out the test for the judicial approval of an authorisation in respect of directed surveillance. The relevant judicial authority must be satisfied that not only were there reasonable grounds for the designated person within the local

authority to believe that using directed surveillance was necessary and proportionate (subsection (3)(a)(i)), but that there also remain reasonable grounds for believing so (subsection (3)(b)). The relevant judicial authority must also be satisfied that any other "relevant conditions" which relate to the authorisation were met (subsection (3)(a)(ii)).

180. New section 32A(4) lists the relevant conditions which must be met if the relevant judicial authority is to approve the granting of an authorisation in respect of directed surveillance. For local authorities in England and Wales (and in Northern Ireland where the authorisation or notice is granted or given for a purpose relating to an excepted or reserved matter) the conditions are: (a) whether the person making the authorisation was of the correct office, rank or position and was accordingly a designated person for the purposes of section 29 of RIPA; (b) whether the authorisation was in breach of any other restrictions imposed by the Secretary of State by virtue of the power at section 30(3); and (c) whether the authorisation or notice satisfied any other conditions set out in an order (subject to the negative resolution procedure) made by the Secretary of State. In relation to conditions (a) and (b), the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) applies. For authorisations granted by public authorities other than local authorities to which the judicial approval requirement may in the future be applied, the relevant conditions are those that will be set out in an order (subject to the negative resolution procedure) made by the Secretary of State.

181. New section 32A(5) sets out the test for the judicial approval of the granting of an authorisation to use CHIS. The relevant judicial authority must be satisfied that there were reasonable grounds for the designated person within the local authority to believe that using a CHIS was necessary and proportionate in that case, and that there remain reasonable grounds for believing so. The relevant judicial authority will also need to be satisfied that when the authorisation was granted there were reasonable grounds for believing, and there remain reasonable grounds for believing, that the arrangements for the source's case satisfied the requirements of section 29(5) of RIPA (which includes arrangements relating to the oversight of the source, the welfare of the source and record keeping) and any additional requirements that have been imposed by order made by the Secretary of State under section 29(7)(b) of RIPA were satisfied. The judicial authority must also be satisfied that the "relevant conditions" which relate to the authorisation were met (subsection (5)(a)(ii)).

182. New section 32A(6) lists the other relevant conditions that must be met if the relevant judicial authority is to approve the granting of an authorisation in respect of the use of a CHIS by a local authority. In the case of an authorisation granted by a local authority in England and Wales (and in Northern Ireland where the authorisation is granted in relation to an excepted or reserved matter), the conditions are: (a) that whether the person granting the authorisation was of the correct office, rank or position and was therefore a designated person within the meaning of section 29 of RIPA; (b) whether the authorisation was in breach of any prohibition imposed by an order made under section 29(7)(a) or any restrictions made by the Secretary of State by virtue of the power at section 30(3); and (c) whether the authorisation or notice satisfied any other conditions that may be set out in an order (subject to the negative resolution procedure) made by the Secretary of State. In respect of the second of these conditions, the Regulation of Investigatory Powers (Juveniles) Order 2010 (SI 2000/2793) imposes certain restrictions where the CHIS is under the age of 18 and the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 (SI 2010/123) imposes certain restrictions to protect information that is legally privileged. In relation to the first and second conditions, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) applies. For public authorities other than local authorities to which the judicial approval requirement may in the future be applied, the relevant conditions are those to be set out in an order (subject to the negative resolution procedure) made by the Secretary of State.

183. New section 32A(7) defines various terms used in new section 32A.

184. New section 32B sets out the procedure for obtaining judicial approval to use directed surveillance or a CHIS.

185. New section 32B(1) provides that the authority to which the relevant person (authorising officer) belongs may apply for approval of the authorisation of the use of directed surveillance or a CHIS by the relevant judicial authority. The relevant person is not required to apply in person.

186. New section 32B(2) provides that notice of such applications for approval need not be given to either the subject of the authorisation or to their legal representatives; this reflects the covert nature of the exercise of the investigatory powers under RIPA.

187. New section 32B(3) allows the relevant judicial authority on refusing an approval of an authorisation to quash that authorisation.

188. *Subsection (2)* amends section 43 of RIPA to make provision for renewals of authorisations for the conduct or use of a CHIS. The renewal may not be approved by the relevant judicial authority unless it is satisfied that a review has been carried out by the authority of the use made of the source and the tasks given to the source within the meaning of section 43(7) of RIPA. The relevant judicial authority must consider the results of the review before approving the renewal.

Part 3: Protection of property from disproportionate enforcement action

Chapter 1: Powers of Entry

Section 39 and Schedule 2: Repealing etc. unnecessary or inappropriate powers of entry

189. *Subsection (1)* confers on the appropriate national authority a power, exercisable by order, to repeal any power to enter land or other premises in either primary or secondary legislation which the Minister considers to be either unnecessary or inappropriate. Such an order may also repeal any "associated power", for example, a power to search or inspect the premises entered into, or to seize material found in such premises; the term is defined in section 46. The power to repeal an associated power may be exercised independently from the power to repeal a power of entry (and vice versa). The term "appropriate national authority" is defined in section 46 as either the Welsh Ministers or a Minister of the Crown; any order made by the Welsh Ministers may only make provision which is within the legislative competence of the National Assembly for Wales.

190. *Subsection (2)* introduces Schedule 2 which directly repeals 15 existing powers of entry that have been identified as unnecessary or that duplicate existing laws. These repeals include a number of antiquated powers of entry relating to agriculture that are no longer required. The list of those powers being repealed also includes a handful of antiquated miscellaneous powers, such as that relating to 'German Enemy Property', which are no longer relevant in today's society.

Section 40: Adding safeguards to powers of entry

191. *Subsection (1)* confers on the appropriate national authority a power, exercisable by order, to add safeguards to any power of entry or associated power. *Subsection (2)* sets out a non-exhaustive list of the safeguards which may be included in such an order. Any such safeguards prescribed in an order would be in addition to (with or without modifications) those already contained in the legislation conferring the power of entry or any associated power. The safeguards which may be prescribed in an order made under this section may include, amongst other things:

- restrictions as to the types of premises in respect of which the power may be exercised. For example, provision could be made to limit the operation of the power to commercial or business premises, or to exclude private dwellings;
- restrictions as to the times at which the power may be exercised. For example, provision could be made to limit the operation of the power to reasonable day time hours;
- a requirement for the power of entry to be subject to an authorisation. This could, for example, be an internal authorisation granted by an officer of a specified minimum seniority within the organisation concerned, or a warrant granted by a court (likely to be a magistrates' court or, in Scotland, a sheriffs' court), or both;
- obligations on the person exercising the power. For example, provision could be made to show the occupier of the premises some form of identification; to provide a written receipt for anything taken from the premises following a search; or to provide specified written information to the occupant (such as in respect of the procedure for making a complaint about the way the power of entry or an associated power was exercised).

Section 41: Rewriting powers of entry

192. *Subsections (1)* and *(2)* confer on the appropriate national authority a power, exercisable by order, to rewrite any powers of entry or associated powers with or without modifications. The powers extend to rewording related enactments. Such an order might consolidate a number of powers of entry exercisable for similar purposes or by a defined category of state officials. Whilst an order made under this section may alter a power of entry or associated power and any safeguard linked to such powers, the combined effect of the changes must be to add to the level of protection afforded by the safeguards when taken together (*subsection (3)*).

Section 42: Duty to review certain existing powers of entry

193. *Subsection (1)* places a duty on each Cabinet Minister to conduct a review of relevant powers of entry and relevant associated powers for which the Minister is responsible. The terms 'relevant powers of entry' and 'relevant associated powers' are defined in *subsection (3)* as those made under a public general Act or statutory instrument made under such an Act. It would, for example, accordingly fall to the Home Secretary to review powers of entry, and associated powers, exercisable by, amongst others, the police and UK Border Agency staff. In conducting such a review the Minister must consider whether, in relation to each power of entry (and associated power), to exercise the order-making powers in sections 39(1), 40 or 41. Each Cabinet Minister is required to prepare a report on the review and lay a copy of the report before Parliament. These reviews must be completed, and the report of each review laid before Parliament, within two years of Royal Assent to this Act. By virtue of *subsection (2)* any failure to review a particular power of entry (or associated power) does not affect the validity of that power.

Section 43: Consultation requirements before modifying powers of entry

194. Before making an order under sections 39(1), 40 or 41 the appropriate national authority must consult with the representatives of persons entitled to exercise the powers of entry (and associated powers) that are to be the subject of such an order. For example, in the case of powers of entry exercised by the police, the Home Secretary would normally consult the Association of Chief Police Officers. The Minister may consult any other persons he or she considers appropriate.

Section 44: Procedural and supplementary provisions

195. *Subsection (1)* provides that an order made under sections 39(1), 40 and 41 may modify any enactment and is to be made by statutory instrument, such an order may include any appropriate incidental, consequential, supplementary, transitory, transitional or saving provisions. The power to make consequential amendments could, for example, be used to repeal any offence which becomes redundant as a result of the repeal of a related power of entry. By virtue of *subsections (2)* and *(4)*, an order made by a Minister of the Crown under sections 39(1), 40 and 41 is subject to the affirmative resolution procedure where it amends or repeals provisions in primary legislation, but is otherwise subject to the negative resolution procedure.

196. *Subsection (3)* disapplies the hybridity procedure should such procedure apply to an order made by the Minister of the Crown under sections 39(1), 40 and 41. The hybridity procedure is explained in paragraph 155.

197. *Subsections (6)* and *(7)* provide that a relevant order made by the Welsh Ministers is similarly subject to the affirmative resolution procedure in the National Assembly for Wales so far as it amends or repeals provisions in primary legislation. Otherwise it is subject to the negative resolution procedure.

Section 45: Devolution: Scotland and Northern Ireland

198. This section provides that an order made under sections 39(1), 40 or 41 may not make provision that would be within the legislative competence of the Scottish Parliament if it were contained within an Act made by the Scottish Parliament, or the Northern Ireland Assembly if it were contained within an Act made by the Northern Ireland Assembly in so far as it deals with a transferred matter.

Section 46: Sections 39 to 46: interpretation

199. Section 46 contains definitions of various terms used in sections 39 to 46. Amongst other things, it adopts the definition of ‘premises’ used in section 23 of the Police and Criminal Evidence Act 1984 (“PACE”).

Section 47: Code of Practice in relation to non-devolved powers of entry

200. *Subsection (1)* places a duty on the Secretary of State to prepare a code of practice in relation to the exercise of powers of entry and associated powers. *Subsection (2)* sets out a non-exhaustive list of matters which may be included in such a code of practice.

201. *Subsection (3)* provides that a code of practice must not make provision in respect of ‘devolved powers of entry and associated powers’ (as defined in *subsection (5)*). A code may make different provisions for different powers of entry and need not contain provision in respect of every power of entry. This ensures that where a power of entry is already subject to an existing code of practice (for example, a code of practice issued under PACE) there is not overlapping guidance in place.

202. *Subsection (4)* requires the Secretary of State, in preparing a code of practice, to consult the Lord Advocate, the representatives of persons entitled to exercise the powers of entry to be covered by the code and such other persons as the Secretary of State considers appropriate.

Section 48: Issuing of code

203. This section sets out the parliamentary procedure for approving the first code of practice made under section 47. *Subsection (1)* requires the Secretary of State to lay before Parliament the proposed code together with a draft order bringing the code into force. Such an order is subject to the affirmative resolution procedure (*subsections (2)* and *(3)*). If the draft order bringing into force the first code of practice is not approved, the

Secretary of State is required to prepare a revised code; the draft order bringing such a revised code into force is again subject to the affirmative procedure (*subsection (4)*).

204. *Subsection (7)* disapplies the hybridity procedure should such procedure apply to the first order made under this section. The hybridity procedure is explained in paragraph 155.

Section 49: Alteration or replacement of code

205. *Subsection (1)* places a duty on the Secretary of State to keep the powers of entry code of practice under review. The Secretary of State may, in the light of such a review, amend the existing code or substitute a new code (*subsection (1)(b)*). *Subsection (2)* requires that in making any alteration to the code or when introducing a new code the Secretary of State must again consult the Lord Advocate, the representatives of persons affected by the code and such other persons as the Secretary of State considers appropriate. *Subsections (3) to (9)* make provision relating to the issuing of a replacement or amended code. In particular, either House of Parliament has 40 days (excluding any period during which Parliament is not sitting for more than four days) in which to pass a resolution refusing to approve the code. If such a resolution is passed then the Secretary of State may prepare another code of practice or amended code of practice for resubmission. Where no resolution is passed, the replacement or amended code will come into force at the end of the 40-day period.

Section 50: Publication of code

206. This section requires the Secretary of State to publish the powers of entry code of practice once approved under section 48, and to publish any subsequent revisions to that code or any replacement code.

Section 51: Effect of code

207. *Subsection (1)* provides that a 'relevant person' must have regard to the code of practice when exercising the powers of entry or associated powers to which the code relates. *Subsection (5)* provides that a 'relevant person' for these purposes is a person specified, or of a description specified, in an order made by the Secretary of State (such an order is subject to the affirmative resolution procedure (*subsection (9)*)). Such an order may provide that a relevant person is only required to have regard to the powers of entry code of practice when discharging specified functions or acting in a specified capacity (*subsections (6)* and *(7)*). 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. Before making such an order the Secretary of State must consult the representatives of the persons to be affected by it and other persons he or she considers appropriate (*subsection (8)*).

208. *Subsection (2)* provides that a failure to adhere to any aspects of the code of practice would not, of itself, render a person liable to civil or criminal proceedings. However, the code of practice is admissible in criminal or civil proceedings (*subsection (3)*) and a court or tribunal may take into account any failure of a relevant authority to comply with the duty to have regard to the code (*subsection (4)*).

Section 52: Sections 47 to 51: interpretation

209. This section applies the definitions of the terms 'power of entry code' contained in section 49(10) and of the terms 'power of entry' and 'associated power' contained in section 46 to the use of those terms in sections 47 to 51.

Section 53 and Schedule 3: Corresponding code in relation to Welsh devolved powers of entry

210. Section 53 introduces Schedule 3 which confers a power on the Welsh Ministers to issue a code of practice about Welsh devolved powers of entry and associated powers. The Schedule makes broadly similar provisions to those contained in sections 47 to 52. The one substantive difference between the two sets of provisions is that section 50 places a duty on the Secretary of State to publish a powers of entry code of practice, whereas under Schedule 3 the Welsh Ministers have a discretion whether or not to issue a code in respect of devolved powers of entry.

Chapter 2 of Part 3: Vehicles left on land

Section 54: Offence of immobilising etc. vehicles

211. *Subsection (1)* makes it a criminal offence to immobilise a motor vehicle by attaching to the vehicle, or to a part of the vehicle, an immobilising device (typically a wheel clamp), or to move (for example, by towing away) or to restrict the movement of a vehicle (for example, by using another vehicle to prevent it being driven away). To be guilty of the offence, a person must undertake one of these actions with the intention of preventing or inhibiting a person entitled to move the vehicle concerned from moving the vehicle. Consequently, a person who moved an obstructively parked vehicle a short distance intending to regain access to his or her property would not be committing the offence in circumstances where he or she did not intend to prevent the driver of the vehicle from subsequently retrieving it. Similarly, the required intention would not be present in the case of a person applying a wheel clamp to his or her own vehicle to prevent theft. The offence does not apply where a person is acting with lawful authority when immobilising, moving or restricting the movement of a vehicle. There are a number of bodies with statutory powers to immobilise or remove vehicles in specified circumstances, including: local authorities when enforcing road traffic contraventions on the public highway or local authority managed car parks; the police when enforcing road traffic contraventions or otherwise removing vehicles that are illegally, obstructively or dangerously parked; the police and local authorities when exercising their powers to remove abandoned vehicles from public and private land; the Department for Transport's Driver and Vehicle Licensing Authority ("DVLA") in respect of vehicles that have no road tax; the Vehicle and Operator Services Agency in respect of vehicles that are not roadworthy; and the police and local authorities when exercising their powers to remove vehicles forming part of an unauthorised traveller encampment. In addition, bailiffs have a mix of statutory and common law powers to immobilise and tow away vehicles for the purposes of enforcing debts (including those arising out of unpaid taxes and court fines).

212. *Subsection (2)* provides that any consent, whether express or implied, given by a person entitled to remove the vehicle to the immobilisation, movement, or restriction of movement, does not constitute lawful authority for the purposes of subsection (1). A driver of a vehicle, by parking in a commercially run car park, may have impliedly accepted the landowner's offer to park (or that of the parking company acting as the landowner's agent). He or she may also, depending on what is advertised at the car park, have impliedly agreed to comply with the terms and conditions advertised, including the parking charges and the associated enforcement mechanism for those charges. However, by virtue of this subsection, the operation of the law of contract as it applies to commercially run private car parks does not confer lawful authority on the landowner or operator of a car park to clamp or tow away a vehicle parked there.

213. Subsection (2) is subject to the exception in *subsection (3)* the effect of which is to exclude from the ambit of the offence the case of a driver who has given express or implied consent (for example, when entering a privately operated car park) to the movement of his or her vehicle being restricted by a fixed barrier. Accordingly, no offence would be committed where a driver was prevented from leaving a car park

because the vehicle's exit was blocked by a fixed barrier which remained in place because the driver had not paid the requisite parking charges (provided the barrier was present when the vehicle was parked, whether or not it only subsequently restricted movement, for example by being lowered into place).

214. *Subsection (4)* contains an exception so that anyone entitled to remove a vehicle cannot commit the subsection (1) offence in respect of that vehicle. This would apply where the owner of a vehicle retrieves a vehicle being used by another person (for example, a car hire company recovering an unreturned vehicle in respect of which the car hire agreement had expired).

215. *Subsection (5)* sets out the maximum penalty for the offence, namely on summary conviction a fine not exceeding the statutory maximum (currently £5,000) and on conviction on indictment an unlimited fine.

Section 55: Extension of powers to remove vehicles from land

216. This section amends section 99 of the Road Traffic Regulation Act 1984 so as to extend the power to make regulations for the police and others to remove vehicles in certain circumstances. Section 99 of the Act enables the Secretary of State to provide in regulations for the removal of vehicles that are illegally, obstructively or dangerously parked or broken down on a road. A road is defined for these purposes as 'any length of highway or any other road to which the public has access, and includes bridges over which a road passes' (section 142 of the Road Traffic Regulation Act 1984). Section 99 of the Road Traffic Regulation Act also enables regulations to be made governing the removal of vehicles that have been abandoned on a road or 'on any land in the open air'. The current regulations made under section 99 include the Removal and Disposal of Vehicles Regulations 1986 (SI 1986/183), as amended. These regulations give the police, local authorities and others the power (not a duty) to remove vehicles in the circumstances described in section 99. The effect of the amendments to section 99 will be to enable regulations to be made which confer a power on the police, local authorities or others to remove vehicles that are illegally, dangerously or obstructively parked on any land (*subsections (2)* and *(3)*). The power to remove abandoned vehicles is similarly extended so that it is no longer restricted to vehicles abandoned 'on any land in the open air', so ensuring that the power could cover places such as an underground car park.

Section 56: Recovery of unpaid parking charges

217. Section 56 gives effect to Schedule 4 which makes provision in certain circumstances for the recovery of unpaid parking related charges from the keeper or the hirer of a vehicle.

Schedule 4: Recovery of unpaid parking charges

218. *Paragraph 1* introduces the scheme as provided for in Schedule 4. The scheme provides that, subject to certain conditions being met, the keeper or the hirer of a vehicle may be made liable for any unpaid parking charge that has arisen as a result of either: the driver of the vehicle having entered into a contract with a landowner and/or another person authorised to require payment of parking charges on the land in question; or, through the driver of the vehicle committing a trespass or other tort on land where parking is prohibited. The scheme is based on the legal analysis that a driver of a vehicle by parking on private land either expressly or implicitly accepts the landowner's offer to park (or that of a parking company acting as the landowner's agent), or prohibition on parking and agrees to comply with any terms and conditions (including any parking charges and the associated enforcement mechanism for those charges) advertised on a notice board at the entrance to and within the land. The driver may commit a trespass by parking on private land without permission or, if the terms and conditions of any agreement which the driver has implicitly accepted are not adhered to, then the driver may be in breach of that agreement. In either situation, whether the existence of a contract can

be established or, alternatively, if the driver can be shown to have committed a tort, the Schedule envisages a situation where the vehicle can be "ticketed" for charges due under the terms of that contract or for the pre-estimated damages resulting from the trespass.

219. Under the current law, parking providers wishing to enforce charges against drivers are able to obtain details of the vehicle keeper from the DVLA if they are able to show "reasonable cause" for wanting the information (so as to satisfy regulation 27(1)(e) of the Road Vehicles (Registration and Licensing) Regulations 2002 (SI 2002/2742)). A parking provider managing parking in accordance with industry best practice has reasonable cause to seek from the DVLA the keeper details of a vehicle in respect of parking related charges that have not been paid. The DVLA requires parking companies requesting keeper details for parking enforcement purposes to be members of an accredited trade association (the British Parking Association's Approved Operator Scheme is the only trade association currently so accredited). Whilst landowners and agents may seek to recover unpaid parking charges from vehicle keepers, as the law is currently understood to stand, any parking contract will be between the driver of a vehicle and the parking provider and any tort is committed by the driver of the vehicle. Accordingly, the keeper may not be liable in law for the charges incurred if he or she was not the driver at the time.

220. *Paragraphs 2* and*3*define various terms used in the Schedule. The scheme applies only to vehicles parked on "relevant land", the definition of which excludes a highway maintainable at public expense and a parking place provided or controlled by a traffic authority. Other land where parking is governed by a statutory scheme including that contained in Part 6 of the Traffic Management Act 2004 (which includes provision for keeper liability) is also excluded from the scheme as set out in this Schedule.

221. *Paragraph 4* provides that the creditor has a right to recover unpaid parking charges from the keeper of the relevant vehicle if the conditions set out in *paragraphs 5*, *6*, *11* and *12* are satisfied. The creditor is not obliged to pursue unpaid parking charges through this scheme and may seek to do so through other means but they may not use the scheme provided for here to secure double recovery of unpaid parking charges (*paragraph 4(6)*), nor will they have the right to pursue the keeper, as opposed to the driver, of the vehicle where they have sufficient details of the driver's identity. The right to reclaim unpaid parking charges from the vehicle keeper does not apply in cases where the vehicle has been stolen before it was parked, (*paragraphs 4(2)* to *(3)*), or in certain circumstances where the vehicle in question was a hire vehicle (paragraph 4(7)). The creditor may not make a claim against the keeper of a vehicle for more than the amount of the unpaid parking related charges as they stood when the notice to the driver was issued (*paragraph 4(5)*).

222. *Paragraph 5* sets out the first condition which is that the creditor must have the right to enforce the requirement to pay unpaid parking charges against the driver of a vehicle but is unable to do so because the creditor does not know the name and current address of the driver.

223. *Paragraph 6* sets out the second condition which is that the creditor must have served the appropriate notices as set out in *paragraphs 7 and 8 or 9*. Paragraph 7 sets out the requirements for a valid a notice to the driver. This must either have been given to the person in charge of the vehicle or affixed to the vehicle whilst it was still located on the land and comply with the requirements of *paragraph 7(2)* which lists the matters that must be set out in the notice, including the total amount of the parking charges payable and the arrangements for the resolution of disputes and complaints that are available. In the event that the notice is not settled by the driver (within the 28 day window provided for under the Schedule), paragraph 8 sets out the requirements which must be followed in order to serve a subsequent notice on the keeper of the vehicle requiring either payment of the unpaid parking charges or the name and address of the driver of the vehicle at the relevant time. In the event that it is not possible to serve an

initial notice on the driver of the vehicle (for example, if parking enforcement is carried out after the event via CCTV), paragraph 9 sets out the requirements which must be adhered to when serving a first notice directly to the keeper of the vehicle.

224. *Paragraph 10* contains a power for the Secretary of State (or the Welsh Ministers) to prescribe in regulations any requirements as to the evidence which must accompany a valid notice to the keeper.

225. *Paragraph 11* sets out the third condition (which applies only to registered vehicles) which is that the creditor has applied to the Secretary of State (in practice, the DVLA) for the name and address of the keeper and that information has been provided.

226. *Paragraph 12* contains a power for the Secretary of State (or the Welsh Ministers) to prescribe in regulations any requirements for the display of notices on relevant land. The fourth condition is that if any such requirements are prescribed, they must have been complied with prior to the period of parking in question.

227. *Paragraph 13* contains provisions which are relevant to vehicle-hire firms who may receive notices under the Schedule as registered keepers of hire vehicles for charges incurred when those vehicles are, or have been, on hire. Paragraph 13 provides that where the vehicle-hire firm provides the creditor with a statement confirming that the vehicle was hired at the relevant time, together with a copy of the hire agreement and a statement signed by the hirer confirming that the hirer agrees to be responsible for all parking charges incurred during the period of hire, it is the hirer of the vehicle who is liable for the unpaid parking charges and not the vehicle-hire firm. *Paragraph 14* sets out the procedure and requirements for the creditor to then serve a further notice on the hirer of the vehicle requesting payment of the unpaid parking charges.

228. *Paragraph 15* provides that the scheme applies to Crown vehicles that are required to be registered with the DVLA and to the keeper of such vehicles. The scheme does not, however, apply to vehicles used for military purposes or that belong to visiting forces.

229. *Paragraph 16* confers a power on the Secretary of State (or the Welsh Ministers) to amend certain provisions in Schedule 4 by order (subject to the affirmative resolution procedure); the relevant provisions are the definition of "relevant land" in *paragraph 3(1)*, and any of the conditions to which the right to claim unpaid parking charges is subject. *Paragraph 17* provides that any regulations made by the Secretary of State (or the Welsh Ministers) under the Schedule are subject to the negative resolution procedure.

Part 4: Counter-terrorism powers

Section 57: Maximum detention period of 14 days

230. Schedule 8 to the Terrorism Act 2000 ("the 2000 Act") makes provision in respect of the treatment of terrorist suspects detained under section 41 of or Schedule 7 to that Act. Paragraph 36(3)(b)(ii) of Schedule 8 provides that the maximum period for which a terrorist suspect may be detained without charge is 28 days from the time of arrest. As originally enacted, Schedule 8 provided for a maximum period of pre-charge detention of seven days. This was increased to 14 days by section 306 of the Criminal Justice Act 2003 ("the 2003 Act") and then to 28 days by section 23 of the Terrorism Act 2006. However, in increasing the maximum period to 28 days, the Terrorism Act 2006 made this period subject to a 'sunsetting' provision. Section 25 of that Act provides that the maximum period of 28 days is subject to renewal by affirmative order for periods up to one year at a time, failing which the maximum period reverts to 14 days. Section 25 operates in such a way that where no order made under subsection (2) is in force, Schedule 8 is modified so as to provide for a maximum period of pre-charge detention of 14 days. The last order made under section 25(2) (The Terrorism Act 2006 (Disapplication of Section 25) Order 2010 (SI 2010/1909)) expired on 24 January 2011. *Subsection (1)* amends paragraph 36(3)(b)(ii) of Schedule 8 to the 2000 Act so as to

make the maximum period of pre-charge detention, as provided for by that Act, 14 days. *Subsection (2)* repeals section 25 of the Terrorism Act 2006 so as to remove the order-making power contained in that provision and as a result, the ability to revert to a maximum period of pre-charge detention of 28 days through that mechanism.

Section 58: Emergency power for temporary extension and review of extensions

231. Section 58 inserts a new paragraph 38 into Schedule 8 to the 2000 Act which provides a new power for the Secretary of State to make an order that will increase the maximum period of detention under Schedule 8 to the 2000 Act, to 28 days. The power to make an order can only be used where the Secretary of State considers it necessary by reason of urgency, and can only be exercised during a period when Parliament is dissolved or in the period before the first Queen's Speech of the new Parliament, (fast track legislation would be introduced should a period of detention of more than 14 days be required at any other time, see paragraph 47 above). This limited order-making power was introduced as a response to a recommendation made in a report (published on 23 June 2011[30]) by the Joint Committee convened to carry out pre-legislative scrutiny of the Draft Detention of Terrorist Suspects (Temporary Extension) Bills. Where an order is made, the maximum period of pre-charge detention under Schedule 8 is extended to 28 days. Any applications for warrants of further detention which would take the period of detention beyond 14 days must be made to a senior judge, and be made with the consent of the Director of Public Prosecutions (in England and Wales), or the Director for Public Prosecutions for Northern Ireland (in Northern Ireland) or the Lord Advocate (in Scotland). *Subsection (2)* provides that an order made under new paragraph 38 must be laid before Parliament as soon as it is reassembled following a general election and that any order will cease to have effect after 20 days if a resolution by both Houses of Parliament is not passed to approve it. By virtue of section 7(1) of the Statutory Instruments Act 1946, in calculating the 20 day period no account is to be taken of any time during which Parliament is dissolved, or prorogued, or during which both Houses are adjourned for more than four days. *Subsection (3)* introduces a requirement for the person appointed as Independent Reviewer of Terrorism Legislation under the Terrorism Act 2006 (or someone on his behalf), to conduct a review of any application for a warrant of further detention which takes the period of detention in respect of an individual or individuals, beyond 14 days.

Section 59: Repeal of existing stop and search powers

232. Section 59 repeals the stop and search powers in sections 44 to 47 of the 2000 Act.

Section 60: Replacement powers to stop and search persons and vehicles

233. *Subsection (1)* repeals section 43(3) of the 2000 Act which requires that searches of persons be carried out by someone of the same sex. This requirement is being repealed to make it the same as other (both non-terrorist and terrorist) stop and search powers which do not include a same sex search requirement. This is because any search will normally be carried out on the street and it is not always practicable to summon an officer of the appropriate gender in a reasonable time.

234. *Subsection (2)* supplements the existing stop and search power in section 43 of the 2000 Act, by providing that where a vehicle is stopped in the course of stopping a person under section 43 (that is, where a constable reasonably suspects a person to be terrorist), the constable may search the vehicle as well as the person. 'Terrorist' is defined in section 40 of the 2000 Act.

235. *Subsection (3)* creates a new stop and search power in respect of vehicles by inserting new section 43A into the 2000 Act. New section 43A provides a power for police to stop and search a vehicle, including its driver, any passengers and anything in or on the

30 http://www.publications.parliament.uk/pa/jt201012/jtselect/jtdetent/161/161.pdf

vehicle, if a constable reasonably suspects the vehicle is being used for the purposes of terrorism. 'Terrorism' is defined in section 1 of the 2000 Act, and section 1(5) provides that a reference in that Act to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation. Anything discovered during a search which the officer reasonably suspects may constitute evidence that the vehicle is being used for the purposes of terrorism, may be seized and retained.

Section 61: Replacement powers to stop and search in specified locations

236. *Subsection (1)* inserts new section 47A into the 2000 Act. New section 47A replaces in part the powers in sections 44 to 46 of the 2000 Act repealed by section 59. The new powers allow a senior police officer (defined in paragraph 14(1) and (2) of new Schedule 6B to the 2000 Act, inserted by Schedule 5 to this Act) to give an authorisation to allow the stop and search of vehicles (including drivers of vehicles, passengers and anything found in or on a vehicle) and pedestrians (including anything carried by a pedestrian), to search for anything that may constitute evidence that a person is a terrorist, or the vehicle is being used for the purposes of terrorism. A constable in uniform may exercise the powers, once authorised, regardless of whether he or she has a reasonable suspicion that he or she will find such evidence in the course of a search. A constable includes a constable of the British Transport Police and Ministry of Defence Police, and the Civil Nuclear Constabulary where an authorisation covers an area where its members have the powers and privileges of a constable. In England and Wales and Northern Ireland, a community support officer may also exercise the powers listed in new section 47A(2)(a) and (d), (3)(b) and (6) (see paragraphs 30 and 31 of Schedule 9 to this Act which amend the Police Reform Act 2002 and the Police (Northern Ireland) Act 2003 respectively). An authorisation can only be given if the person giving it reasonably suspects that an act of terrorism will take place and reasonably considers that the authorisation of the powers is necessary to prevent such an act and that the area or place specified in the authorisation are no greater than is necessary and the duration of the authorisation is no longer than is necessary.

237. *Subsection (2)* introduces Schedule 5 which inserts new Schedule 6B into the 2000 Act.

Schedule 5: Replacement powers to stop and search: Supplementary Provisions

238. Schedule 5 inserts a new Schedule 6B into the 2000 Act which makes further provision about authorisations and searches in specified areas or places, as created by the new section 47A.

239. Paragraph 1 of new Schedule 6B states that a constable searching a person in public under powers given by the new section 47A, cannot require that person to take off more than headgear, footwear, outer coat, jacket or gloves.

240. Paragraph 2 provides that a person or vehicle can be detained for as long as is reasonably required to search the person or vehicle, at or near to the place where the person or vehicle is stopped.

241. Paragraph 3 places a duty on a senior police officer who has made an authorisation orally under new section 47A, to confirm it in writing as soon as reasonably practicable.

242. Paragraph 4 requires that if a pedestrian or vehicle is stopped under new sections 47A(2) or (3) and the pedestrian or driver of the vehicle requests a statement that they were stopped by virtue of those sections, then a written statement must be provided, as long as it is requested within 12 months of the stop taking place.

243. Paragraph 5 states that an authorisation given under new section 47A has effect from the time it is given and ends at the time or date specified in the authorisation, subject to the following paragraphs of the Schedule.

244. Paragraph 6 provides that individual authorisations cannot be in place for any longer than 14 days.

245. Paragraph 7 places a requirement on the senior police officer who has given an authorisation, to inform the Secretary of State as soon as reasonably practicable (sub-paragraph (1)). If the Secretary of State does not confirm the authorisation within 48 hours, it ceases to have effect (sub-paragraph (2)). If an authorisation is not confirmed, and ceases to have effect by virtue of sub-paragraph (2), it does not affect the lawfulness of anything carried out under the authorisation before it ceased to have effect (sub-paragraph (3)), including searches and seizures. The Secretary of State may amend the authorisation when confirming it, by shortening its duration or limiting the geographical extent of the authorisation (sub-paragraph (4)).

246. Paragraph 8 gives the Secretary of State a power to cancel an authorisation at any time.

247. Paragraph 9 confers a power on a senior police officer to cancel an authorisation, shorten its duration or reduce its geographical extent (sub-paragraph (1)). If an authorisation has already been confirmed by the Secretary of State under paragraph 7 when a senior police officer cancels it or amends it, the amended authorisation does not require further confirmation from the Secretary of State (sub-paragraph (2)).

248. Paragraph 10 provides that if an authorisation is given by a senior officer in the Civil Nuclear Constabulary, then the power conferred by the authorisation is only available to members of that Constabulary at times and places where they have the powers and privileges of a constable.

249. Paragraph 11 provides that a new authorisation may be given, regardless of whether a previous authorisation exists, has been cancelled or expired.

250. Paragraph 12 provides that a senior police officer (other than those of the British Transport Police, Ministry of Defence Police or Civil Nuclear Constabulary), may give an authorisation which covers internal waters adjacent to an area or place which is covered by an authorisation, or a place within those internal waters. 'Internal waters' means waters in the United Kingdom which are not part of a police area.

251. Paragraph 13(a) provides that where an authorisation includes more than one area or place, it may specify different end dates for those areas or places, and where it does so, the powers of the Secretary of State or the senior police officer to shorten the duration of the authorisation includes the power to shorten any one or more of those periods. Paragraph 13(b) provides that if an authorisation is given which covers more than one area or place, then the Secretary of State or senior police officer may remove areas or places from the authorisation under their powers to restrict the geographical extent of an authorisation in paragraph 7(4)(b) or 9(1)(c) respectively.

252. Paragraph 14 defines a number of terms used in new Schedule 6B.

Section 62: Code of Practice

253. This section, which inserts new sections 47AA to 47AE into the 2000 Act, makes provision for a code of practice for terrorism stop and search powers. New section 47AA places a duty on the Secretary of State to prepare a code of practice about the powers in sections 43 and 43A of the 2000 Act (stop and search with reasonable suspicion), and those created by new section 47A of the 2000 Act. New section 47AB makes provision for the code to be brought into force by order, subject to the affirmative resolution procedure. New section 47AC requires that the code is kept under review; any amendments to the code or replacement code are subject to the same parliamentary procedure as provided for in new section 47AB. New section 47AD requires that the code and any altered versions are published. New section 47AE(1) requires a police officer (or police community support officer) to have regard to the code when exercising the powers to which it relates and explains the effect of the code. New section 47AE(2) provides that a failure to adhere to any aspects of the code of practice would not, of itself,

render a person liable to civil or criminal proceedings. However, the search powers code is admissible in criminal or civil proceedings (new section 47AE(3)) and a court or tribunal may take into account any failure by a police officer (or community support officer) to comply with the duty to have regard to the code (new section 47AE(4)).

Section 63: Stop and search powers in relation to Northern Ireland

254. Section 63 introduces Schedule 6 which amends the stop and search power for munitions and transmitters in relation to a constable.

Schedule 6: Stop and search powers: Northern Ireland

255. *Paragraph 1* amends paragraph 4 of Schedule 3 to the Justice and Security (Northern Ireland) Act 2007 ("the 2007 Act") which provides, in subsection (1), that a constable or member of Her Majesty's forces on duty (an "officer") may stop a person in a public place in Northern Ireland to search that person for munitions held unlawfully and wireless apparatus. In exercising this power, the officer does not need to have reasonable suspicion for doing so.

256. *Paragraphs 1(2)* and *(3)* replace the word "officer" with "a member of Her Majesty's forces who is on duty". A constable can no longer stop and search a person in a public place without reasonable suspicion but the existing power for the military to stop and search a person remains unchanged.

257. *Paragraph 1(4)* inserts new sub-paragraph (4) into Schedule 3 to the 2007 Act so that a constable can search a person whom he or she reasonably suspects to have munitions unlawfully with him or her or to have wireless apparatus with him or her regardless of whether he or she is in a public place or not (currently the reasonable suspicion requirement only applies where the person is not in a public place).

258. *Paragraph 2* inserts a new paragraph 4A into Schedule 3. New paragraph 4A(1), read with the definitions in new paragraph 4A(8), provides that a senior officer of the Police Service of Northern Ireland of at least the rank assistant chief constable may authorise the use of the stop and search power without reasonable suspicion in a specified area if the senior police officer reasonably suspects that the safety of any person might be endangered by the use of munitions or wireless apparatus. The authorisation can be given only if the senior police officer reasonably considers that it is necessary to prevent that danger and the area or place specified in the authorisation is no greater than is necessary and the duration of the authorisation is not longer than is necessary.

259. New paragraph 4A(2) states that any constable is authorised to stop and search an individual in the area or place specified in the senior police officer's authorisation.

260. New paragraph 4A(3) specifies that a constable may exercise the power conferred by the authorisation only for the purpose of ascertaining whether the person is carrying munitions unlawfully or wireless apparatus.

261. New paragraph 4A(4) provides that the power conferred by the authorisation may be exercised whether or not the constable reasonably suspects the person has such munitions or wireless apparatus.

262. New paragraph 4A(5) states that a constable searching a person in public under new paragraph 4A, cannot require that person to remove clothing with the exception of headgear, footwear, outer coat, jacket or gloves.

263. New paragraph 4A(6) provides that a person can be detained for as long as is reasonably required to carry out the search of the person at, or near to where he or she was stopped.

264. New paragraph 4A(7) places a duty on a senior police officer who has made an authorisation orally under new paragraph 4A, to confirm it in writing as soon as reasonably practicable.

265. New paragraph 4B states that an authorisation given under new paragraph 4A has effect from the time it is given and ends at the time or date specified in the authorisation subject to new paragraphs 4C to 4G of the Schedule.

266. New paragraph 4C provides that an authorisation cannot specify a date or time which is more than 14 days after the date the authorisation is made.

267. New paragraph 4D places a requirement on the senior officer who has made an authorisation under new paragraph 4A to inform the Secretary of State of it as soon as reasonably practicable (sub-paragraph (1)). If the Secretary of State does not confirm the authorisation within 48 hours of it having been made, it ceases to have effect (sub-paragraph (2)). If an authorisation is not confirmed and ceases to have effect by virtue of sub-paragraph (2), it does not affect the lawfulness of anything carried out under the authorisation before it ceased to have effect (sub-paragraph (3)). The Secretary of State may, when confirming an authorisation, shorten its duration or reduce its geographical extent (sub-paragraph (4)).

268. New paragraph 4E provides that the Secretary of State may cancel an authorisation at any time.

269. New paragraph 4F confers a power on a senior police officer to cancel an authorisation, shorten its duration or reduce its geographical extent (sub-paragraph (1)). If an authorisation has already been confirmed by the Secretary of State under paragraph 4D when a senior police officer cancels it or shortens its duration or reduces its geographical extent, the amended authorisation does not require further confirmation from the Secretary of State (sub-paragraph (2)).

270. New paragraph 4G provides that a new authorisation can be given regardless of whether a previous authorisation continues in force, has expired or has been cancelled.

271. New paragraph 4H provides that a senior police officer may give an authorisation which covers either the whole of or part of Northern Ireland or all or part of the internal waters adjacent to it or any combination of them (sub-paragraph (1)). 'Internal waters' are defined as waters in the United Kingdom that are adjacent to Northern Ireland (sub-paragraph (2)). Sub-paragraph (3) makes provision for authorisations which specify more than one area or place and provides that such an authorisation can specify more than one end date or time (consequently the powers of the Secretary of State or a senior officer to substitute earlier end dates or times also apply) and that the Secretary of State and a senior officer, when substituting a more restricted area or place under new paragraphs 4D(4)(b) and 4F(1)(c) respectively, may remove an area from the authorisation.

272. New paragraph 4I deals with circumstances in which a decision of a senior officer, or of the Secretary of State, to give, vary or cancel an authorisation is challenged in any legal proceedings. Under sub-paragraph (2) the Secretary of State may certify that the interests of national security are relevant to the decision and the decision was justified. Such a certificate can be appealed to the tribunal established under section 91 of the Northern Ireland Act 1998 ('the National Security Certificates Appeals Tribunal'). The Tribunal has the power to uphold or quash a certificate. The procedural rules which are currently used by the Tribunal make provision for sensitive material to be considered in closed session and for the appointment of special advocates.

Part 5: Safeguarding vulnerable groups, criminal records etc.

Chapter 1: Safeguarding of vulnerable groups

Section 64: Restriction of scope of regulated activities: children

273. Section 64 amends the definition of 'regulated activity relating to children' which is set out in Part 1 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006

("SVGA"). Part 1 of Schedule 4 to the SVGA specifies what work a person is barred from doing if he or she is included in the children's barred list. A person may be included in that list as a result of committing certain offences or following a decision by the Independent Safeguarding Authority ("ISA") that the individual presents a risk of harm to children. A person can be barred in England and Wales by virtue of being included in a corresponding children's barred list in Northern Ireland or Scotland. The overall effect of section 64 is to reduce the scope of work that barred individuals are prohibited from doing.

274. Broadly speaking, the activities specified in Part 1 of Schedule 4 to the SVGA comprise paid and unpaid work that involves certain close interaction with or (in a specified place) the opportunity for contact with children. It also includes work carried out by individuals occupying certain positions ('office-holders') whose functions relate to services provided for, or in relation to, children. Any work falling within Part 1 of Schedule 4 must not be carried out by an individual who is included in the children's barred list.

275. The amendments made to the SVGA by this section provide that regulated activity relating to children no longer includes the following:

- Any supervised teaching, training or instruction of children, unless any such activity takes place in a specified place such as a school, children's home or a children's centre (with the exception of work in specified settings carried out by supervised volunteers, which is to be removed from the scope of regulated activity);
- The provision of any care or supervision of children by a person where the provision of such care or supervision is being supervised by another unless, once again, it takes place in a specified place (as above). Further exceptions to this are where certain types of personal care or health care are provided to children, in which case not only will such types of care fall within the definition of regulated activity (even if supervised), they will also fall within that definition if such care is provided only on occasion. This is because the requirement in Schedule 4 to the SVGA for any activity mentioned above to be undertaken regularly (for it to be a regulated activity) is removed in relation to the provision of such personal care or health care;
- The provision of any legal advice to a child;
- Any paid work that is carried out in a specified place, which gives the worker the opportunity to have contact with children and which is of an occasional or temporary nature (excluding any teaching, training, instruction, care for or supervision of or advice to children that is carried out on an occasional or temporary basis). This would, for example, mean that work carried out in a school by maintenance or building contractors is no longer a regulated activity relating to children but that any teaching by supply/locum teachers would continue to be a regulated activity;
- The work of officials of the Children and Family Courts Advisory and Support Service (CAFCASS) and their Welsh equivalents and the work of office-holders in various governance-related or senior management roles, for example a school governor, a local authority director of children's services, and the Children's Commissioner for England;
- The work of inspectorates in England, for example inspectors of schools, children's homes and childminding in England;
- Inspection work by the Care Quality Commission;
- The day-to-day management or supervision, on a regular basis, of any type of work referred to above that is removed from regulated activity; and

- Work that is a regulated activity solely because it takes place in a hospital and provides the opportunity for an individual to have contact with children.

276. This section also brings within the meaning of 'health care' for the purposes of Part 1 of Schedule 4 to the SVGA, the provision of first aid to a child by anyone acting on behalf of an organisation established to provide first aid (new paragraph 1(1D) of Schedule 4). This means that the work of organisations such as St John's Ambulance is added to the scope of regulated activity. This would not however encompass a designated first-aider in a workplace.

Section 65: Restriction of definition of vulnerable adults

277. Section 59(1) of the SVGA currently defines vulnerable adults by reference to certain settings or by receipt of certain services and certain specific status. Regulated activity relating to vulnerable adults is currently defined in section 59 of, and Parts 2 and 3 of Schedule 4 to, the SVGA. The definition is widely drafted to cover, for example, "any form of care for or supervision of vulnerable adults" (paragraph 7(1)(b) of Schedule 4) or "any form of assistance, advice or guidance…wholly or mainly for vulnerable adults" (paragraph 7(1)(c)). Regulated activity was also qualified by 'a frequency condition' (paragraph 7(1)).

278. *Subsection (1)* repeals section 59 of the SVGA and *subsection (2)* inserts a new definition into section 60(1) (interpretation) of the SVGA so that 'vulnerable adult' means any person aged 18 or over for whom an activity (that is, a 'regulated activity'), as defined in paragraph 7(1) (read with paragraphs 7(2) to (3E)) of Schedule 4 to the SVGA, is provided. An adult is vulnerable at the time they are being provided an activity specified to be a regulated activity relating to adults. Section 66 (see paragraph 280 below) amend the definition of regulated activity relating to vulnerable adults.

Section 66: Restriction of scope of regulated activities: vulnerable adults

279. Section 66 replaces the definition of 'regulated activity' relating to vulnerable adults (existing paragraphs 7(1) to (3) of Schedule 4 to the SVGA). *Subsection (2)* replaces the paragraphs 7(1) to (3) with new sub-paragraphs (1) to (3E). These new sub-paragraphs redefine regulated activity in relation to vulnerable adults to include:

- the provision of health care treatment in any setting by a health care professional, or by a person acting under the direction or supervision of a health care professional such as a health care assistant in a hospital or care home. This includes first aid provided by organisations such as St John's Ambulance, as is the case for children;

- the provision of relevant personal care in any setting to a person who needs the care because of age, illness or disability. Relevant personal care is defined at new sub-paragraph (3B) as physical care such as assistance with eating, drinking, toileting, washing and dressing; prompting, together with supervision, for those activities, where such prompting and supervision are necessary for their execution; and any training, instruction, advice or guidance in relation to the performance of those activities to a person in need of it by reason of age, illness or disability (for example, a person given training on how to, for example, clean their teeth following a stroke);

- the provision of relevant social work by a social worker to clients or potential clients. Relevant social work is defined at new sub-paragraph (3C) as having the meaning in section 55(4) of the Care Standards Act 2000;

- the provision of assistance, in relation to general household matters, to a person who requires it because of age, illness or disability. This is defined as day to day assistance with managing the person's cash, paying bills, or shopping;

- the provision of assistance to a person where there is a formal arrangement in place which allows a person to make welfare and/or financial decisions on behalf of another person of a kind specified in new sub-paragraph (3E);

- the transportation provided because of a person's age, illness or disability. Regulations will set out the specific circumstances when transportation will be a regulated activity relating to vulnerable adults, and intended to cover various forms of transportation by hospital porters, emergency care staff, and transport for the purpose of a person's health or social care needs arranged by or on behalf of the care provider or voluntary organisation.

280. *Subsection (3)* removes from the definition of regulated activity an activity in a care home provided for vulnerable adults falling within paragraph 7(4) of Schedule 4 to the SVGA. Workers who provide health or personal care or any other regulated activity to care home residents will fall within the revised definition in new paragraph 7(1) of Schedule 4 to the SVGA. Save for a consequential amendment, paragraph 7(5) of Schedule 4 is retained, so line managers with regular day to day management or supervision of a person carrying out a regulated activity as mentioned in new paragraph 7(1) (for example, care home managers) are still within scope.

281. *Subsection (5)* removes the inspection of providers of English local authority social services (other than local authorities) from the definition of regulated activity relating to vulnerable adults. The inspection of providers of Welsh local authority social services continues to fall within that definition.

282. *Subsection (6)* removes from the definition of regulated activity certain inspection functions of the Care Quality Commission.

283. *Subsections (7)* and *(8)* remove persons in specified roles and offices from the definition of regulated activity, including a member of a relevant local government body, local authority chief executives, charity trustees and the proprietors or managers of regulated establishments or agencies.

284. *Subsection (9)* removes the period condition in respect of regulated activity for vulnerable adults. This means that a person providing a regulated activity within the meaning of paragraph 7(1) of Schedule 4 to the SVGA will need only do so once to come within the scope of the revised Scheme.

Section 67: Alteration of test for barring decisions

285. This section amends Schedule 3 to the SVGA which sets out how someone may be referred by the Secretary of State to the ISA and included in the children's barred list (Part 1 of Schedule 3) or the adults' barred list (Part 2 of Schedule 3).

286. *Subsection (1)* relates to the children's barred list and amends the provisions (set out in paragraphs 1(2) and (3) of Schedule 3 to the SVGA) for the automatic barring of persons who meet the prescribed criteria. The prescribed criteria are set out in regulations (the Safeguarding Vulnerable Groups Act 2006 (Prescribed Criteria and Miscellaneous Provisions) Regulations 2009: SI 2009/37 (as amended) and refer to circumstances where individuals have been convicted or cautioned for a serious criminal offence, which give rise to a clear indication of risk to children or vulnerable adults. Subsection (1) substitutes new sub-paragraphs 1(2) and 1(3) for those in Schedule 3 to the SVGA to provide that when the Secretary of State has reason to believe that a person meets the criteria for automatic barring (without representations) by the ISA as prescribed in the Prescribed Criteria Regulations, the Secretary of State must refer that person to the ISA. If the ISA is satisfied that paragraph 1 applies to a person (whether or not that person was referred to them by the Secretary of State), the ISA must include that person in the children's barred list.

287. *Subsection (2)* substitutes new sub-paragraphs (2) to (8) of paragraph 2 of Schedule 3 to the SVGA for the existing sub-paragraphs (2) to (4) which govern "automatic bars with representations". These bars are based on criminal convictions or cautions which, whilst not providing such a clear indication of risk as the criteria falling under paragraph 1 of Schedule 3, are still serious and raise the presumption of a risk of harm to children or vulnerable adults. These offences are also set out in the Prescribed Criteria Regulations. New paragraphs 2(2) to (8) of Schedule 3 amend the arrangements for the referral of these cases to the ISA by the Secretary of State so as to limit the requirement for the Secretary of State to make referrals to the ISA and limiting the ISA bars to those engaged in 'regulated activity' and those who have been or might in the future be engaged in regulated activity. New paragraph 2(4) requires the ISA to seek representations from an individual who has committed such an offence, prior to reaching a decision on whether to place them on the children's barred list. If no such representations are received within the prescribed time period, it requires the ISA to place the person on the barred list. If representations are received, then the ISA must consider whether it is appropriate to include the individual in the barred list. New paragraphs 2(6) and (8) limit the application of such bars to those who are engaged, have been engaged or might in the future be engaged in regulated activity.

288. *Subsections (3)* and *(4)* provide the same limitation of the bar to those who are engaged in, have been engaged in or might in the future be engaged in, regulated activity, in respect of persons referred to the ISA on the grounds of behaviour (paragraph 3 of Schedule 3 to the SVGA) or risk of harm (paragraph 5 of Schedule 3) in relation to children. These provisions ensure that only those who are engaged in regulated activity, have been engaged in regulated activity or might in the future be engaged in such activity can be placed on the children's barred list.

289. *Subsections (5)* to *(8)* make the same changes as subsections (1) to (4) in respect of persons referred to the ISA or placed on the adults barred list (paragraphs 7 to 11 of Schedule 3 to the SVGA).

Section 68: Abolition of controlled activity

290. Section 68 repeals sections 21 and 22 of the SVGA which define 'controlled activity' relating to children and vulnerable adults; it also repeals section 23 of the SVGA which enables regulations to be made governing the steps that employers must take when considering allowing a person to engage in a controlled activity. Under the SVGA 'controlled activity' consists of specified types of activities that are ancillary in nature to work that falls within regulated activity. A person barred from engaging in regulated activity may do work that is a controlled activity. Regulations made under section 23 of the SVGA require an employer to check if a person is barred from regulated activity before permitting them to engage in a controlled activity. The purpose of this is to ensure that employers are able to assess if the individual in question is suitable for the controlled activity position and, if so, whether any safeguards need to be put in place. This section abolishes the concept of 'controlled activity'.

Section 69: Abolition of monitoring

291. This section repeals sections 24 to 27 of the SVGA which, had they been brought into force, would have made provision for the monitoring by the Secretary of State of persons engaged in regulated activity, broadly those individuals who are working closely with, or applying to work closely with, children or vulnerable adults or whose work otherwise falls within the current definition of 'regulated activity'. The monitoring system would have required the majority of individuals engaged in or seeking to engage in regulated activity to make an application to the Secretary of State to be monitored. Applications to the Secretary of State which revealed any criminality information would have been referred to the ISA for consideration for barring and any person barred could not become or remain "subject to monitoring". Monitoring of applicants would have involved the collation of any updated material (such as new convictions

or cautions) in relation to people registered with the Secretary of State for the purpose of being monitored, and referral of any new information to the ISA so that it could consider whether that person should be included on either or both of the barred lists. This section abolishes those requirements and any other requirements relating to the proposed monitoring scheme.

Section 70: Information for purposes of making barring decisions

292. *Subsection (1)* amends paragraph 19 of Schedule 3 to the SVGA which provides the ISA with the power to obtain relevant police information in relation to any individual's case it is considering. As currently drafted, paragraph 19(1) of Schedule 3 requires the police and others to provide the ISA with information about convictions and cautions relating to a person to whom any of paragraphs 1 to 5 or 7 to 11 of Schedule 3 "applies". Subsection (1) alters this test so that the duty to provide ISA with conviction data operates where any of the relevant paragraphs of Schedule 3 "applies or appears to apply". This is because it may not be clear to the ISA at the time of the referral whether the criteria for automatic or discretionary barring have been satisfied. Subsection (1) also introduces a requirement for a "reasonable belief" test to be applied by those holding criminality information in respect of the relevance of information to be provided, consistent with the revised test to be applied in relation to police intelligence information disclosed on enhanced criminal record certificates (see section 82).

293. *Subsection (2*) substitutes a new sub-paragraph (2) of paragraph 20 of Schedule 3 to the SVGA for the existing one. New paragraph 20(2) provides that when the Secretary of State refers a person to the ISA under paragraphs 1, 2, 7 or 8 of Schedule 3 (that is, because the prescribed criteria for the automatic barring provisions is triggered) and (in the case of referrals under paragraphs 2 and 8) the Secretary of State has reason to believe the person is engaging in, has engaged in, or might in the future engage in regulated activity, then the Secretary of State is also obliged to send the ISA certain information. This information will be prescribed details of a relevant matter, that is, prescribed details of convictions or cautions. This is further tempered by the ability for the type of conviction or caution information to be limited by regulations so that not all conviction or caution information will be provided by the Secretary of State to the ISA.

Section 71: Review of barring decisions

294. Section 71 (which inserts a new paragraph 18A into Schedule 3 to the SVGA) enables the ISA to review an individual's inclusion in either of the barred lists and, in certain circumstances, to remove that person from the list. The circumstances are set out in new paragraph 18A(3).

Section 72: Information about barring decisions

295. *Subsection (1)* replaces sections 30 to 32 of the SVGA with new sections 30A and 30B. Sections 30 and 32 would have enabled employers and others registering a legitimate interest in a person who was subject to monitoring under section 24 of the SVGA, to be informed should that person become barred. Section 24 is repealed by section 69.

296. New section 30A introduces arrangements for an interested party to obtain from the Secretary of State, on application, information indicating whether a person is barred from regulated activity. Such information may only be provided with the person's consent. Eligibility to apply for such information is governed by Schedule 7 to the SVGA, and includes, for example, regulated activity providers. New section 30A(5) provides for a fee in respect of such an application, and new section 30A(7) enables the Secretary of State to determine the form, manner and contents of the application. This would result in a reactive notification system where the interested party is told, upon request, whether a particular individual is barred.

297. New section 30B enables persons mentioned in Schedule 7 to the SVGA to register an interest in persons engaged in regulated activity. It requires the Secretary of State

to notify the registered person should an individual become barred from regulated activity. Registration requires the consent of the individual engaged in regulated activity and, for this purpose, any consent given by an individual for a barred list check under section 30A suffices for consent for registration under new section 30B. New section 30B(8) provides for a fee to be charged for this service and new section 30B(10) enables the Secretary of State to determine the form, manner and content of any application. This fee will be set at a level necessary to recover the costs of this service. This would result in a proactive notification system whereby the interested person is automatically told when a particular individual is barred.

298. *Subsection (2)* amends section 33(3) of the SVGA to provide for registration to be periodically renewed and for registration to cease if it is not renewed.

299. *Subsections (4)* and *(5)* replace the existing power to add entries to the table in paragraph 1 of Schedule 7 to the SVGA with a power to amend or repeal entries in that table, or add new entries to it.

300. *Subsection (6)* repeals the provision set out in paragraph 3(1)(b) of Schedule 7 to the SVGA, which enables the Ministry of Defence to carry out barred list checks on those supervising persons aged under 18 working for the armed forces.

Section 73: Duty to check whether person barred

301. This section inserts new section 34ZA into the SVGA. New section 34ZA(1) places a duty on a 'regulated activity provider' to ascertain whether a person is barred before permitting that person to engage in regulated activity.

302. New section 34ZA(2) places a similar duty on a personnel supplier who provides persons to work in regulated activity (for example, a provider of agency teachers or care home workers) to ensure that any personnel they provide, knowing that they will be engaging in regulated activity, are not barred.

303. New sections 34ZA(3) to (6) provide that the duties to check are met in particular where the provider has obtained information under new section 30A; obtained an enhanced criminal record certificate (under Part 5 of the Police Act 1997) in respect of regulated activity (which will indicate whether the person is barred); or checked such a certificate and received up-date information in relation to that certificate as provided for under section 83.

304. New section 34ZA(7) enables the Secretary of State by regulations (subject to the negative resolution procedure) to disapply the duties in subsections (1) and (2) in respect of persons of a prescribed description.

Section 74: Restrictions on duplication with Scottish and Northern Ireland barred lists

305. Section 74 prevents duplication between the barred lists held in respect of England and Wales, Northern Ireland, and Scotland. It provides that the ISA must not include a person in the barred lists (which apply in England and Wales) if it knows that the person is included in a corresponding list. A corresponding list is one which is maintained under the law of Scotland or Northern Ireland, and which is specified by order of the Secretary of State as corresponding to either the children's barred list or the adults' barred list maintained by the ISA.

306. This section also enables the ISA to remove a person from the barred lists if they know that a person is included in a corresponding list maintained in Northern Ireland or Scotland.

Section 75: Professional bodies

307. This section amends the duties on professional bodies by combining the effects of sections 43 and 44 of the SVGA.

308. Section 41 of the SVGA places an obligation upon professional bodies (also known as keepers of registers), for example the General Medical Council, to provide the ISA with information (of a prescribed sort) about a person whom it may be appropriate to include in a barred list, if certain conditions are met. *Subsection (1)* replaces the obligation to provide this information with a power to do so and removes the requirement that the information must be of a prescribed sort. This means that the professional body can provide any relevant information to the ISA, if the referral criteria are met.

309. The changes made by *subsection (3)* ensure that the ISA is under an obligation to inform a professional body that someone on their register is on a barred list. The ISA must also provide the keeper of a register with any information upon which it relied in coming to that decision and which the ISA considers both to be relevant to the functions of the professional body and appropriate to disclose to that body. The amendments to the SVGA also enable a professional body to apply to the ISA for barred list information on an *ad hoc* basis. The ISA may provide to the professional body any information that is relevant to them; this does not have to be in relation to a barred person. The amendments further provide for a professional body to apply to the Secretary of State to be proactively notified if anyone on their register becomes barred.

310. The provisions ensure that neither the ISA nor the Secretary of State is under any obligation to provide information if the ISA (or the Secretary of State, as the case may be) is satisfied that the professional body already has that information.

Section 76: Supervisory authorities

311. Section 76 makes similar amendments to the provision of information to supervisory authorities (for example Her Majesty's Chief Inspector of Schools in England). *Subsection (1)* replaces the duty on a supervisory authority to provide information to the ISA that may be relevant to a barring decision with a power to do so. This subsection and *subsection (2)* also make several amendments to section 47 of the SVGA which are consequential upon the abolition of monitoring. *Subsection (3)* ensures that any obligation to provide children's barred list information to any supervisory authority does not apply if the Secretary of State is satisfied that the supervisory authority already has that information. *Subsection (4)* makes similar amendments in respect of individuals on the adults' barred list. *Subsection (5)* alters the obligation on the ISA to provide the supervisory authority with information to a power to do so and limits the supervisory authority's ability to request information under section 50 of the SVGA to a situation in which the information is required in connection with one of their functions.

Section 77: Minor amendments

312. *Subsection (1)* repeals uncommenced amendments to the SVGA made by the Policing and Crime Act 2009 ("the 2009 Act"). *Paragraph (a)* omits section 87(2) of the 2009 Act, which would have required the notification to employers of an intention by the ISA to bar an individual, prior to the receipt of representations and a final decision as to whether to place a person on the barred lists. *Paragraph (b)* omits section 89(6) of the 2009 Act which amended the power of the Secretary of State to examine convictions or cautions in connection with criteria for the referral of individuals to the ISA under Schedule 3 to the SVGA; such referrals will now be governed by the revised arrangements in section 67.

313. *Subsection (2)* amends section 39(1) of the SVGA so as to replace the duty on a local authority to provide information to the ISA which may be relevant to a barring decision with a power to do so.

314. *Subsection (3)* amends section 50A(1) of the SVGA which governs the provision of information to the police by the ISA. The amendment enables the ISA to provide police forces with information for the purposes of recruitment to the police service and for other reasons which may be prescribed (in addition to the existing grounds of the prevention, detection and investigation of crime, or the apprehension and prosecution of offenders).

315. *Subsection (4)* places on the ISA a duty to provide, on request to any chief officer of police, information as to whether a person is on a barred list and either or both of the entire barred lists. This applies for any of the reasons for which information can be provided to the police, including the new reasons introduced by subsection (3).

316. Subsection (4) also provides the ISA with a power to inform the Secretary of State, in their capacity as being responsible for Her Majesty's Prison Service, or the Probation Service, about information which the ISA reasonably believes to be relevant, provided that it is for the purpose of protecting children or vulnerable adults. This subsection also places on the ISA a duty to provide to the Secretary of State (in practice, the Prison Service) or the Probation Service, on request, information about whether a person is on a barred list, provided that it is for the purpose of protecting children or vulnerable adults.

317. Section 64 (see paragraphs 274 to 277) specifies that certain activities that would generally constitute regulated activity relating to children will no longer be within the scope of regulated activity if the person carrying out that activity is subject to regular, day to day supervision by another person who is carrying out regulated activity. *Subsection (6)* of section 77 inserts new paragraph 5A of Schedule 4 to the SVGA, which provides that the Secretary of State must publish guidance to assist regulated activity providers and personnel suppliers in deciding whether supervision is of such a kind that the person being supervised would not be engaging in regulated activity relating to children. New paragraph 5A(2) provides that the Secretary of State must consult the Welsh Ministers before issuing that guidance; and new paragraph 5A(4) requires that regulated activity providers and personnel suppliers must, in exercising any of their functions under the SVGA, have regard to that guidance.

Section 78: Corresponding amendments in relation to Northern Ireland

318. Section 78 introduces Schedule 7, which amends the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 ("SVGO"). The SVGO provides the framework for the vetting and barring scheme in Northern Ireland.

Schedule 7: Safeguarding of vulnerable groups: Northern Ireland

319. *Paragraph 1* replicates the provisions in section 64, which limit the scope of regulated activity in relation to children. However, unlike in England and Wales, the following activities are retained within the scope of regulated activity:

- the work of education, health, social care and justice inspectorates;
- the activities of Guardians Ad Litem; and
- the function of a controller appointed in respect of a child under Article 101 of the Mental Health (NI) Order 1986.

320. A children's hospital is also being retained as a specified establishment (there is only one dedicated children's hospital in Northern Ireland) and accordingly persons working in such an establishment would come within the scope of regulated activity.

321. *Paragraph 2* replicates the changes to the definition of vulnerable adults as provided for in section 65.

322. *Paragraph 3* replicates the provisions in section 66, which limit the scope of regulated activity in relation to vulnerable adults, with some adjustment to reflect differences in Northern Ireland legislation. *Paragraph 4* replicates the provisions in section 67 (alteration of test for barring decisions) so that decision-making by the ISA will be conducted consistently across England, Wales and Northern Ireland.

323. *Paragraph 5* abolishes controlled activity in Northern Ireland in line with the position in England and Wales provided for in section 68 and *paragraph 6* replicates section 69 by abolishing monitoring under the vetting and barring scheme in Northern Ireland.

324. *Paragraphs 7* and *8* replicate the provisions of sections 70 and 71, which will alter the way barring decision-making by the ISA will be undertaken and reviewed. *Paragraph 9* replicates section 72 (information about barring decisions) by inserting new Articles 32A and 32B into the SVGO. These new Articles make statutory provision for the introduction of new reactive and proactive barred list notification mechanisms in Northern Ireland.

325. *Paragraph 10* places a statutory duty on employers, volunteer managers and personnel suppliers to check whether an individual is barred prior to being permitted to engage in regulated activity with children or vulnerable adults in Northern Ireland, as is set out in section 73.

326. *Paragraph 11* makes reciprocal provision to section 74 by preventing duplicate inclusion in Northern Ireland, England and Wales, and Scotland barred lists and enabling the ISA to remove a person from a barred list if it knows that a person is included in a corresponding barred list.

327. *Paragraphs 12* and *13* replicate the provisions of sections 75 and 76 respectively. These paragraphs provide for information flows between the ISA and professional bodies and regulation and inspection bodies in Northern Ireland. The requirement for professional bodies and regulation and inspection bodies to refer matters to the ISA is also replaced with a power to refer.

328. *Paragraph 14* replicates section 77 by making equivalent minor amendments to the SVGO and omitting section 90(2) of the 2009 Act. Included in the minor amendments is provision for the police, prisons and Probation Board for Northern Ireland to obtain barred list information from the ISA.

Chapter 2 of Part 5: Criminal Records

Section 79: Restriction on information provided to certain persons

329. *Subsection (1)* repeals section 93 of the 2009 Act which, if commenced, would have inserted a new section 112(2A) into the 1997 Act. That section would have required the Secretary of State to send a copy of a criminal conviction certificate (which includes only any unspent convictions) to any named employer in the application. This change is in line with the changes made in *subsection (2)*.

330. Subsection (2) repeals sections 113A(4) and 113B(5) and (6) of the 1997 Act. When a person applies for a standard certificate or an enhanced certificate, the Criminal Records Bureau ("CRB") issues the relevant certificate not only to the applicant but also, by virtue of sections 113A(4) and 113B(6) of the 1997 Act, sends a copy of the certificate to the registered body which countersigned the application. A registered body will normally be the applicant's employer or prospective employer or other organisation acting on behalf of an employer. The simultaneous issue of the certificate to an applicant and a registered body does not afford the applicant the opportunity to review and, if necessary, challenge the information contained in a certificate before it is released to an employer. The repeal of sections 113A(4) and 113B(6) removes the provisions that require a copy of a certificate to be sent to the registered body so that the certificate is issued to the applicant only, allowing the applicant to make appropriate representations

to the CRB regarding the information released without the disputed information already having been seen by the employer.

331. Section 113B(5) of the 1997 Act enables sensitive (non-conviction) information which might be relevant to an employer to be provided to a registered body without it being copied to the applicant. Such a procedure is adopted, for example, where the police are engaged in an ongoing criminal investigation and the premature release of the relevant information to an applicant for an enhanced criminal record certificate might compromise that investigation. The repeal of section 113B(5) removes the statutory obligation to disclose the relevant information to the registered body in these circumstances. However, it would remain open to the police, using their common law powers to prevent crime and protect the public, to pass such information to a potential employer where they considered it justified and proportionate.

332. *Subsection (3)* inserts a new section 120AC into the 1997 Act that will allow registered bodies to continue to be able to track online the progress of an application for a criminal record certificate or an enhanced criminal record certificate, including whether it has been issued and for the registered body to be informed that the certificate does not contain any relevant information when that is the case (in effect, that the certificate is 'clear').

333. Subsection (3) also inserts a new section 120AD into the 1997 Act to provide that the CRB must in certain circumstances send a copy of the certificate to the registered body. Those circumstances are when the new updating service has advised that a new certificate should be applied for, such a certificate has been applied for, and the applicant has not, within the prescribed period, sent a copy of it to the relevant person. A copy would be sent to the registered body only if a request is made within the prescribed period and none of the prescribed circumstances apply.

Section 80: Minimum age for applicants for certificates or to be registered

334. Under sections 112(1), 113A(1), 113B(1), 114(1) and 116(1) of the 1997 Act, the Secretary of State is required to issue a criminal conviction certificate, criminal record certificate, enhanced criminal record certificate, criminal record certificate (Crown employment) and enhanced criminal record certificate (judicial appointments and Crown employment) respectively to any individual who makes an application in the prescribed manner and form and pays the prescribed fee - that is, the Secretary of State has no discretion to refuse an application submitted by a person below a certain age. *Subsection (1)* amends the provisions of the 1997 Act so that the duty on the Secretary of State to issue the relevant certificate only applies where the applicant is aged 16 years or over.

335. *Subsection (2)* amends section 120(4) of the 1997 Act so that registered persons who countersign applications for criminal record certificates and enhanced criminal record certificates must be aged 18 years or over.

Section 81: Additional grounds for refusing an application to be registered

336. Section 81 amends the arrangements governing the CRB to extend the provision determining the grounds on which the CRB can refuse to register an organisation as a "Registered Body" (that is, a body responsible for the processing and the counter-signature of applications for criminal record certificates) to include the power to refuse to register an organisation that has previously been removed from the register as a result of a breach of the CRB Conditions of Registration.

Section 82: Enhanced criminal record certificates: additional safeguards

337. Under section 113B(4) of the 1997 Act an enhanced criminal record certificate may include, in addition to details of any convictions or cautions, other information which, in the opinion of a relevant chief officer of police might be relevant to an employer's

decision on whether the applicant is suitable for the role concerned. *Subsection (1)* of section 82 (taken together with *subsection (3)*) makes two material changes to section 113B(4). First, it amends the test to be applied by a chief officer when determining whether additional, non-conviction information should be included in an enhanced criminal record certificate. In place of the current test of information which, in the opinion of the chief officer 'might be relevant' and ought to be included in the certificate, subsection (1) substitutes a higher test of information which the chief officer 'reasonably believes to be relevant' and which in the chief officer's opinion ought to be included in the certificate.

338. The second change to section 113B(4) affected by subsection (3) relates to the chief officer of police whom the Secretary of State is required to approach to ascertain whether he or she holds any relevant non-conviction information on the applicant for a certificate. At present, such an approach must be made to the chief officer of every relevant police force. A 'relevant police force' is defined in Regulation 10 of the Police Act 1997 (Criminal Records) Regulations 2002 (SI 2002 233 as amended) as any police force which holds information about the applicant (whether conviction or non-conviction information); there may be two or more such police forces which will independently come to a decision about what, if any, non-conviction information about the applicant might be relevant and ought to be included in the enhanced criminal records certificate. By virtue of the amendments to section 113B(4) and (9) made by *subsection (1)(a)* and subsection (3) the Secretary of State will be able to approach any 'relevant chief officer'; in this way one chief officer can be assigned to take a decision on the disclosure of non-conviction information held by any number of police forces. It would be open to the Secretary of State to appoint one chief officer to act as the relevant chief officer in respect of all applications for enhanced criminal record certificates or to appoint a small number of chief officers, for example, one per region, to undertake the role on behalf of all forces.

339. *Subsection (2)* inserts a new subsection (4A) into section 113B of the 1997 Act. New section 113B(4A) enables the Secretary of State to issue guidance to relevant chief officers about the discharge of their functions under section 113B(4) to provide relevant non-conviction information about an applicant for an enhanced criminal record certificate; a relevant chief officer is required to have regard to any such guidance.

340. Under section 117 of the 1997 Act, an applicant in receipt of a criminal conviction certificate, criminal record certificate or enhanced criminal record certificate who disputes the accuracy of the information contained in such a certificate may make an application in writing to the Secretary of State for a new certificate. The Secretary of State may consider the application and, if of the opinion that the information is inaccurate, will issue a new certificate. *Subsection (4)* of section 82 inserts new subsection (1A) into section 117, which allows parties other than the applicant to make such an application, which must also be in writing.

341. *Subsection (5)* inserts new section 117A into the 1997 Act, which provides that a dispute can be raised in relation to an enhanced criminal record certificate in relation to the non-conviction information supplied by a relevant chief officer. The person may apply to the independent monitor (appointed under section 119B of the 1997 Act) to determine whether that information is relevant or ought to be included in the certificate. The independent monitor must ask an appropriate chief officer of police to review whether the information concerned is relevant and ought to be included on the certificate. If, following that review, the independent monitor decides that the information either is not relevant or should not be included in the certificate, the independent monitor must inform the Secretary of State, who must issue a new certificate which excludes that information. In exercising their review functions, both the chief officer and the independent monitor must have regard to the guidance published by the Secretary of State under section 113B(4A) of the 1997 Act.

Section 83: Up-dating certificates

342. This section inserts new section 116A into the 1997 Act. One of the main features of the current CRB system is that a criminal record certificate or an enhanced criminal record certificate is a snapshot in time showing only what conviction and other relevant information was recorded on police and law enforcement databases as of the date a certificate was issued. This means that the reliance an employer can place on the information contained in a certificate diminishes with the lapse of time following the issue of a certificate, which impedes the 'portability' of a certificate between roles (that is, the ability of an employee or volunteer to present a certificate obtained for one job or voluntary position to a second employer or voluntary organisation).

343. New section 116A of the 1997 Act introduces a procedure for updating certificates on a continuous basis. An applicant for a criminal conviction certificate, criminal record certificate or enhanced criminal record certificate may subscribe to the updating arrangements at the time an application for a certificate is submitted and thereafter re-subscribe to those arrangements on an annual basis. The update arrangements will only be put in place in respect of an applicant for a certificate and thereafter renewed on payment of an initial fee and subsequently of an annual fee to be prescribed by regulations made under new section 116A(4) and (5) (by virtue of section 125 of the 1997 Act such regulations are subject to the negative resolution procedure). The annual fee will be set at a level necessary to recover the costs of the service and will be offset by the removal of the need to make repeat applications for a criminal record certificate. Under the update arrangements the CRB will not, as such, provide any new conviction or other relevant information to the subscriber to the updating arrangements. Instead, by virtue of the definition of 'up-date information' in new section 116A(8), in response to a request for update information, the CRB will advise the person making the request (which can be the applicant, or any person authorised by the applicant who is entitled to see that information) either that there is no new information that would be included on a new certificate or that a new certificate should be applied for (which would imply that a new certificate would contain new information).

Section 84: Criminal conviction certificates: conditional cautions

344. Section 84 amends section 112(2) of the 1997 Act which details the content of a criminal conviction certificate. Such a certificate includes the details of any convictions unspent under the terms of the Rehabilitation of Offenders Act 1974. The amendment to section 112(2) provides that a criminal conviction certificate must also include details of any unspent conditional cautions. A conditional caution is an out of court disposal whereby an offender avoids being prosecuted for an offence by admitting his or her guilt and agreeing to comply with certain conditions designed to rehabilitate the offender or provide reparation to the victim; under the Rehabilitation of Offenders Act 1974 a conditional caution becomes spent after three months. Section 112 of the 1997 Act is not in force in England and Wales.

Section 85: Inclusion of cautions etc. in national police records

345. Section 85 amends section 27 of the Police and Criminal Evidence Act 1984 ("PACE") so that cautions, reprimands and warnings are recorded on the Police National Computer ("PNC") in exactly the same way as convictions. The PNC needs to hold all relevant records when applications for criminal record certificates and enhanced criminal record certificates are made so that relevant matters can be disclosed. This section will give the same statutory authority for putting cautions etc on the PNC as already exists for convictions

Section 86: Out of date references to certificates of criminal records

346. Section 86 amends section 75 of the Data Protection Act 1998, which provides that section 56 of that Act, which in turn would make it an offence for an employer or

prospective employer to require a person to supply details of any convictions or cautions in respect of that person held by the police (otherwise known as 'enforced subject access'), cannot be commenced until criminal conviction certificates, criminal record certificates and enhanced criminal record certificates are all available under the 1997 Act. The amendments to section 75 replace out of date references to sections 113 and 115 of the 1997 Act (which were repealed by the Serious Organised Crime and Police Act 2005). The replacement provisions for sections 113 and 115 are now sections 113A and 113B which provide for criminal record certificates and enhanced criminal record certificates respectively.

Chapter 3 of Part 5: The Disclosure and Barring Service

Section 87: Formation and constitution of DBS

347. *Subsections (1)* and *(2)* establish a new body, called the Disclosure and Barring Service ("DBS"). The DBS is intended to combine the current functions of the ISA, in respect of safeguarding vulnerable groups, and of the CRB in respect of providing criminal record certificates. *Subsection (3)* gives effect to Schedule 8, which makes further provision about the constitution and governance of the DBS.

Schedule 8: Disclosure and Barring Service

348. *Paragraph 1* provides that the DBS shall consist of a chair and other members appointed by the Secretary of State, some of whom are expected to have relevant knowledge or experience of child protection or the protection of vulnerable adults. Before appointing the chair or members of the DBS, the Secretary of State is required to consult the Welsh Ministers and a Northern Ireland Minister. *Paragraph 2* provides that an appointment of a member of DBS may not be for more than five years, although reappointment is possible, and sets out the procedures by which an appointed member may resign or may be removed from office. *Paragraph 3* makes provision for the remuneration of members.

349. *Paragraphs 4* and *5* deal with the appointment and remuneration of the chief executive and other staff to the DBS. By virtue of *paragraph 20* the Secretary of State may appoint the first chief executive of the organisation.

350. *Paragraphs 6* to *8*enable the DBS to delegate any of its functions to its members, staff, or a committee of members and/or staff and to delegate non-core functions to a person who is neither an appointed member nor a member of staff. For these purposes, 'core function' is defined as: decisions about whether somebody should be included in or removed from a barred list; consideration of representations made by an individual under Schedule 3 to the SVGA relating to a decision to include them in a barred list; or any function falling under Part 5 of the 1997 Act which is specified in an order by the Secretary of State. Such an order is subject to the negative resolution procedure.

351. *Paragraph 9* requires the DBS, following consultation with the Secretary of State, to publish a business plan at the beginning of each financial year, and *paragraph 10* requires it to publish an annual report on the exercise of its functions.

352. *Paragraph 11* allows for the Secretary of State to make payments to the DBS and *paragraph 12* makes provisions about the annual accounts of the DBS including in respect of the auditing of such accounts by the Comptroller and Auditor General.

353. *Paragraph 13* allows the Secretary of State to issue written guidance to the DBS on the exercise of its functions, to which DBS must have regard. *Paragraph 14* allows the Secretary of State to issue, vary or revoke written directions to the DBS, to which the DBS must comply in relation to any of its functions, except for decisions about including a person in or removing a person from a barred list, or consideration of representations from a person about their inclusion in such a list.

354. *Paragraphs 15* to *19* make supplementary provisions covering the status of DBS as a non-Crown body; its ability to use information obtained in relation to one of its functions for others of its functions; payments made in connection with maladministration; incidental powers; and the authentication of documents to be submitted in evidence.

Section 88: Transfer of functions to DBS and dissolution of ISA

355. *Subsection (1)* of section 88 provides that the Secretary of State may, by order, transfer any function of the ISA to the DBS. *Subsection (2)* provides that the Secretary of State may by order transfer to the DBS any function of the Secretary of State in connection with Part 5 of the 1997 Act (the criminal record certificate functions of the CRB); the SVGA (the CRB's functions in connection with the safeguarding of vulnerable groups); and the SVGO (under which the CRB has equivalent functions to those under the SVGA). *Subsection (3)* allows the Secretary of State by order to dissolve the ISA.

Section 89: Orders under section 88

356. *Subsection (1)* specifies that orders made under section 88 transferring functions to the DBS or abolishing the ISA must be made by statutory instrument. Such an order may make consequential amendments to any enactment; for example, the dissolution of the ISA would require the replacement of legislative references to 'ISA' with 'DBS'. By virtue of *subsections (2)* and *(3)* an order made under section 88 is subject to the affirmative resolution procedure where it amends or repeals provisions in primary legislation, but is otherwise subject to the negative resolution procedure. *Subsection (4)* disapplies the hybridity procedure should such procedure apply to an order made under section 88. The hybridity procedure is explained in paragraph 154.

Section 90: Transfer schemes in connection with orders under section 88

357. Section 90 sets out that the Secretary of State, in connection with an order made under section 88, may make a scheme for the transfer of property, rights or liabilities of the ISA or the Secretary of State (in practice, the CRB). *Subsection (3)* lists supplementary, incidental and transitional provision that may be made by a transfer scheme. These include making provision the same as, or similar to, the TUPE regulations (the Transfer of Undertakings (Protections of Employment) Regulations 2006 (S.I. 2006/246 as amended)). *Subsection (8)* specifies that a transfer scheme may provide for an employee of the ISA or an individual employed in the civil service (in practice, the CRB) to become an employee of the DBS; and that such a scheme may provide that an individual's contract of employment with the ISA or their terms of employment in the civil service will have effect, subject to any necessary modifications, as the terms of that person's contract of employment with the DBS.

358. *Subsection (6)* provides that a transfer scheme may either be included in an order made under section 86 or be a standalone document; in the latter case the scheme must be laid before Parliament.

Section 91: Tax in connection with transfer schemes

359. Section 91 provides a power for the Treasury to make an order (subject to the negative resolution procedure in the House of Commons) providing for the tax consequences of the transfer scheme set out in section 90.

Chapter 4 of Part 5: Disregarding certain convictions for buggery etc.

Section 92: Power of Secretary of State to disregard convictions or cautions

360. *Subsection (1)* provides that a person convicted of, or cautioned for, an offence under:

- section 12 of the Sexual Offences Act 1956 Act ("the 1956 Act") for the offence of buggery,
- section 13 of the 1956 Act for the offence of gross indecency between men, or
- section 61 of the Offences against the Person Act 1861 or section 11 of the Criminal Law Amendment Act 1885 (which contained the corresponding pre-1956 offences).

may apply to the Secretary of State (in practice, the Home Secretary) to have the conviction or caution disregarded.

361. By virtue of section 101(3) to (7), these provisions also cover persons with a conviction for a corresponding offence under military service law, or for the inchoate offences of attempting, loitering with intent, conspiring to commit, or inciting the commission of, an offence of buggery or gross indecency; or aiding, abetting, counselling or procuring the commission of an offence of buggery or gross indecency.

362. *Subsection (2)* provides that a caution or conviction can only be disregarded if the conditions set out in *subsections (3)* and *(4)* are both met.

363. Subsection (3) sets out the first condition, which is that it appears to the Secretary of State that the other person involved in the conduct which amounted to the original offence consented to it and was aged at least 16 years old at the time. The offence must also be one which would not fall within the provisions of section 71 of the Sexual Offenders Act 2003 (that is, sexual activity in a public lavatory) as the intention is that these provisions should only apply to behaviour that is no longer criminal. (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.)

364. Subsection (4) sets out the second condition, namely that the Secretary of State has given notice to the applicant of the decision to disregard the conviction or caution; such notice takes effect 14 days after that notice has been given.

365. The effect of a relevant conviction or caution being designated as a disregarded conviction or caution is explained in sections 95 to 98 *(subsection (5)*).

Section 93: Applications to the Secretary of State

366. *Subsection (1)* provides that an application under section 92 has to be made in writing.

367. *Subsection (2)* sets out the information that must be contained in an application.

368. *Subsection (3)* provides that an applicant may supply additional information to evidence that his conviction satisfies the first condition in section 92, namely that the relevant offence involved consensual gay sex with another person over the age of 16.

Section 94: Procedure for decisions by the Secretary of State

369. *Subsection (1)* requires the Secretary of State in coming to a decision on an application to consider the evidence supplied by the applicant, together with any available relevant police, prosecution or court records of the investigation and prosecution of the offence in question.

370. *Subsection (2)* provides that oral hearings will not be held when deciding whether or not to accept an application; in effect the Secretary of State will come to a decision on the basis of the written information available (subject to section 92).

371. *Subsections (3)* and *(4)* require the Secretary of State to record in writing the decision on an application and to notify the applicant of that decision in writing.

Section 95: Effect of disregard on police and other records

372. *Subsection (1)* provides that where a conviction or caution is disregarded, the Secretary of State must direct the relevant data controller to delete the details of the disregarded caution or conviction from all official records. The term 'relevant data controller' is defined in *subsection (5)* augmented by an order made under that subsection; in most cases this will be the chief officer of police of the force which investigated the offence.

373. *Subsection (2)* provides that notice of deletion can be given at any time once the Secretary of State has made a decision to disregard a conviction or caution, but that deletion will not be effective until the applicant has been informed and 14 days have elapsed since that notification.

374. *Subsection (3)* requires that, subject to subsection (2), the data controller must delete the relevant records as soon as reasonably practicable.

375. *Subsection (4)* provides that the data controller must notify the applicant in writing that deletion has taken place.

Section 96: Effect of disregard for disclosure and other purposes

376. *Subsection (1)* provides that a person with a disregarded conviction or caution is to be treated in law as if he had not committed the offence or been subject to any legal proceedings in respect of the offence (that is, he had not been charged with or prosecuted for the offence or convicted, cautioned or sentenced for the offence) .

377. *Subsection (2)* provides that details of disregarded cautions and convictions cannot be used in any judicial proceedings (as defined in section 98) nor, in any such proceedings, can the individual be asked about or be required to answer questions about any disregarded conviction or caution or any circumstances ancillary to it (see section 98).

378. *Subsection (3)* provides that questions put to a person in any other context (for example, by a prospective employer) asking about that person's past convictions or cautions are not to be treated as including any reference to a disregarded conviction or caution and that failure to provide details of such a disregarded matter will not lead to any liability on the part of the individual.

379. *Subsection (4)* provides that any obligation under any law or other agreement to disclose offences will not apply to such disregarded convictions or cautions.

380. *Subsection (5)* provides that a disregarded caution or conviction is not grounds for dismissal from any office, employment, occupation or profession, nor can it prejudice an individual in any such connection.

Section 97: Saving for Royal pardons etc.

381. This section preserves the power of Her Majesty, under the Royal prerogative, to issue a pardon, commute a sentence or quash a conviction. Accordingly, a person with a disregarded conviction or caution might still receive a Royal pardon in respect of the offence despite the operation of section 96.

Section 98: Section 96: supplementary

382. *Subsection (1)* defines the term 'proceedings before a judicial authority' for the purpose of section 96.

383. *Subsections (2)* and *(3)* define the terms 'circumstances ancillary to a conviction' and 'circumstances ancillary to a caution' respectively for the purpose of section 96.

Section 99: Appeal against refusal to disregard convictions or cautions

384. This section provides for a right of appeal to the High Court against a decision by the Secretary of State not to grant an application for a relevant conviction or caution to become a disregarded conviction or caution (*subsection (1)*). On hearing such an appeal, the High Court cannot hear any new evidence and must reach a decision on the basis of the evidence available to the Secretary of State (*subsection (2)*). If the appeal is granted, the High Court must make an order to the effect that the relevant conviction or caution is to be treated as a disregarded conviction or caution; such an order takes effect after 14 days (*subsections (3)* and *(5)*). There is no further appeal from the High Court's decision (*subsection (6)*).

Section 100: Advisers

385. S*ubsection (1)* enables the Secretary of State to appoint independent advisers to advise on an application from a person under section 93. The advisers can be supplied with such information as is relevant to enable them to undertake their function (*subsection (2)*). The decision on the application will rest with the Secretary of State, who can accept, or not, the advice provided. *Subsection (3)* provides for the payment of expenses and allowances to the advisers.

Section 101: Interpretation: Chapter 4

386. This section defines various terms used in this Chapter.

Part 6: Freedom of information and data protection

Section 102: Release and publication of datasets held by public authorities

387. Section 102 amends the Freedom of Information Act 2000 ("FOIA") which currently provides for access to information held by public authorities.

388. *Subsection (2)* amends section 11 of the FOIA (means by which communication to be made). *Paragraph (a)* inserts a new subsection (1A) which provides that where a request is made for information that is a dataset, or which forms part of a dataset, held by the public authority, and the applicant requests that information be communicated in an electronic form, then the public authority must, as far as is reasonably practicable, provide the information to the applicant in an electronic form that is capable of re-use, in other words a re-usable format.

389. There is no absolute duty for datasets to be provided in a re-useable format as it is recognised that, in some instances, there may be practical difficulties in relation to costs and IT to convert the format of the information. A re-usable format is one where the information is available in machine-readable form using open standards which enables its re-use and manipulation. If the applicant does not want to have the dataset communicated in electronic form, because for example, he or she wants the dataset in hard copy only, then the new duty in section 11(1A) will not arise. However, the public authority would still need to comply with the preference expressed, by virtue of the existing duty in section 11(1)(a) of the FOIA, and must provide the dataset in hard copy so far as it is reasonably practicable to do so.

390. *Paragraph (b)* amends section 11(4) by providing that the discretion which a public authority has in relation to the means by which communication of the information is to be made (which is already subject to the duty in section 11(1) of the FOIA) is now additionally subject to the new duty in section 11(1A).

391. *Paragraph (c)* of subsection (2) inserts new subsection (5) and provides for the definition of "dataset" for the purposes of the FOIA. The definition makes it clear that a dataset is a subset of information within the meaning of the FOIA. The definition provides that a dataset is a collection of information held in electronic form where all

or most of the information meets the criteria set out in the following paragraphs of the new section 11(5).

392. The new subsection (5)(a) requires that the information in a dataset has to have been obtained or recorded by a public authority for the purpose of providing the authority with information in connection with the provision of a service by that authority or the carrying out of any other function of the authority.

393. New subsection (5)(b) requires that the information is factual in nature and (a) is not the product of interpretation or analysis other than calculation, in other words that it is the 'raw' or 'source' data; and (b) provides that it is not an official statistic within the meaning given by the Statistics and Registration Service Act 2007 ("SRSA 2007"). Official statistics have been excluded from the definition of datasets as the production and publication of official statistics is provided for separately in the SRSA 2007.

394. New subsection (5)(c) requires that the information within datasets has not been materially altered since it was obtained or recorded. Datasets which have had 'value' added to them or which have been materially altered, for example in the form of analysis, representation or application of other expertise, would not fall within the definition for the purposes of new subsection (5). Examples of the types of datasets which meet the definition, though not a comprehensive list, will include datasets comprising combinations of letters and numbers used to identify property or locations, such as postcodes and references; datasets comprising numbers and information related to numbers such as spend data; and datasets comprising text or words such as information about job roles in a public authority.

395. *Subsection (3)* inserts new sections 11A and 11B into the FOIA which provide for the new duty to make a dataset available for re-use and the charging of fees. New section 11A(1) provides for the four criteria which must be met for the new section to apply: (a) that a person must have made a request for a dataset; (b) that the dataset requested includes a 'relevant copyright work'; (c) that the public authority is the only owner of the 'relevant copyright work', in other words that it is not jointly owned with another party or that it is not owned in whole or in part by a third party; and (d) that the public authority is communicating the relevant copyright work to the requester under the FOIA, in other words that the dataset requested is not being withheld under one of the exemptions provided for in the FOIA.

396. New section 11A(2) provides that when communicating such a dataset to an applicant, the public authority must make the dataset available for re-use in accordance with the terms of a specified licence. New sections 11A(3) to (7) make provision for the charging of fees by public authorities for making datasets available for re-use. New subsection (3) provides that a public authority may charge a fee by virtue of regulations made under new section 11B and new subsection (4) preserves existing statutory powers for public authorities to charge a fee. New subsection (5) provides that where a public authority intends to charge a fee, it must give the applicant a "re-use fee notice", which states the amount of the fee which must be paid before the dataset is available for re-use. New subsection (6) provides that where the public authority has given the applicant a re-use notice, it is not required to make the dataset available for re-use until the fee is paid in accordance with the notice; and new subsection (7) provides that if a public authority is exercising any existing statutory power to charge, the authority may combine the re-use fee notice with any other notice in accordance with the relevant statutory power being exercised.

397. New section 11A(8) adds definitions of "copyright owner", "copyright work", "database", "database right", "owner", "relevant copyright work", and "the specified licence" to section 11A of the FOIA. The definition of a "relevant copyright work" excludes a "relevant Crown work" and a "relevant Parliamentary work" which are separately defined.

398. Crown owned works are excluded from the requirement on public authorities to make datasets available for re-use under the terms of a licence specified by the Secretary of State. This is because the Controller of Her Majesty's Stationery Office, who is appointed by letters patent from the Queen to manage Crown owned works, already has the authority to require these works and databases to be made available for re-use under the terms of a licence.

399. Parliamentary owned works and databases are excluded from the requirement on public authorities to make such datasets available for re-use because it would not be appropriate to make Parliament subject to a direction of the Secretary of State as new section 11A of the FOIA would in effect do by way of the specified licence in the code of practice under section 45 of the FOIA.

400. New section 11B makes further provision about the charging of fees by public authorities for making datasets (containing relevant copyright works) available for re-use. Subsection (1) confers a power on the Secretary of State to make regulations (subject to the negative resolution procedure) about the charging of fees in connection with making the datasets available for re-use in response to requests under the FOIA and publication schemes. Subsections (2) and (3) set out what the regulations may prescribe, such as when a fee may or may not be charged and how much that fee might be.

401. *Subsection (4)* amends section 19 (publication schemes) of the FOIA. *Paragraph (a)* inserts new subsections (2A) to (2F) into section 19 of the FOIA. Under new section 19(2A), publication schemes must include a requirement for the public authority to publish any dataset it holds, which is requested by an applicant, and any updated version of a dataset, unless the authority is satisfied that it is not appropriate for the dataset to be so published (new subsection (2A)(a)). It requires public authorities, where reasonably practicable, to publish any dataset under new subsection (2A)(a) in an electronic form which is capable of re-use (new subsection (2A)(b)). Subject to new subsection (2B), it also requires public authorities to make any relevant copyright work (if the authority is the only owner) available for re-use in accordance with the terms of the specified licence. New subsections (2B) to (2F) mirror new section 11A(2) to (7) by making equivalent provision in respect of publication schemes for the charging of fees by public authorities for making datasets (where they contain relevant copyright works) available for re-use.

402. *Paragraph (b)* of subsection (4) inserts a new subsection (8) into section 19 of the FOIA which provides definitions of "copyright owner", "copyright work", "database", "database right", "owner", "relevant copyright work" and "the specified licence". The definition of a "relevant copyright work" excludes a "relevant Crown work" and a "relevant Parliamentary work" which are separately defined.

403. *Subsection (5)* amends section 45 of the FOIA (issue of code of practice). *Paragraph (a)* amends the list in section 45(2) of the FOIA, which sets out the matters that must be included in the code of practice made under that section, to insert a new requirement for the code of practice to include provision relating to the disclosure by public authorities of datasets held by them. *Paragraph (b)* sets out the different provisions relating to the re-use and disclosure of datasets that may, in particular, be included in the code of practice under section 45 of the FOIA. *Paragraph (c)* amends section 45(3) of the FOIA so as to provide for the possibility of making more than one code of practice under section 45, each of which makes different provision for different public authorities.

404. *Subsection (6)* inserts into section 84 of the FOIA, which defines the terms used in that Act, a definition of the new term "dataset".

Section 103: Meaning of "publicly-owned company"

405. This section amends section 6 of the FOIA to widen the definition of "publicly-owned company".

406. *Subsection (2)* amends section 6(1) of the FOIA to provide that, as well as companies wholly owned by the Crown, any government department or a single public authority, those wholly owned by one or more bodies from the wider public sector or owned by any such body or bodies in conjunction with the Crown or government departments are also subject to the FOIA. Currently section 6(1) of the FOIA only applies to bodies wholly owned by the Crown, any government department or another single public authority.

407. *Subsection (3)* replaces the current section 6(2) of the FOIA to define when a company is owned by the Crown, the wider public sector, or a combination of both. For a company to be wholly owned by the Crown every member must be a Minister of the Crown, a government department or a company owned by the Crown; or a person acting on behalf of any of these. For a company to be wholly owned by the wider public sector every member must be a relevant public authority or company wholly owned by the wider public sector; or a person acting on behalf of either. For a company to be wholly owned by the Crown and wider public sector at least one member must be a Minister of the Crown, a government department, a company wholly owned by the Crown, or a person acting on behalf of one of these; at least one member must be a relevant public authority, a company wholly owned by the wider public sector, or a person acting on behalf of one of these; and all of its members must fall within these two categories. This has the effect that companies wholly owned by the Crown (including government departments) or any combination of public authorities listed in Schedule 1 to the FOIA (subject to *subsection (4)*) are subject to its provisions, as are companies owned by the Crown and any combination of relevant public authorities. Examples of bodies to which the FOIA will be extended include waste disposal companies and purchasing organisations wholly owned by a number of local authorities.

408. Subsection (4) amends section 6(3) of the FOIA to define "relevant public authority". All public authorities listed in Schedule 1 to the FOIA are relevant public authorities except those listed only in relation to particular information. Companies owned entirely or in part by public authorities listed only in relation to particular information are not publicly-owned companies for FOIA purposes. Government departments are excluded from the definition of a relevant public authority on account of their being part of the Crown.

Section 104: Extension of certain provisions to Northern Ireland bodies

409. *Subsection (1)* repeals section 80A of the FOIA and paragraph 6 of Schedule 7 to the Constitutional Reform and Governance Act 2010 which excluded Northern Ireland bodies from provisions in the FOIA relating to the disclosure of historical records and communications with the Royal Family.

410. As a result Northern Ireland bodies will be subject to the amendments made to sections 2(3) and 37(1)(a) of the FOIA about information relating to communications with the Royal Family and Household. The Constitutional Reform and Governance Act 2010 substituted five categories of communication for those previously set out in section 37(1)(a). These are communications:

- with the Sovereign (new paragraph (a));
- with the heir to the Throne or the second in line to the Throne (new paragraph (aa));
- with a person who has subsequently acceded to the Throne or become heir to, or second in line to, the Throne. This provides an exemption for information which relates to communications with such a person from the date they accede to the Throne or become heir or second in line to the Throne. The exemption also applies to all relevant information created before that date. Should that person cease to be the Sovereign, heir to or second in line to the Throne otherwise than by death and remain a member of the Royal Family then paragraph (ac) will apply to information relating to communications with that person created on or after the date of that change (new paragraph (ab));

- with members of the Royal Family who do not themselves fall within paragraphs (a) to (ab) other than when those communications are made or received on behalf of the persons referred to in paragraphs (a) to (ab) (new paragraph (ac)); and
- with the Royal Household other than where those communications are made or received on behalf of the persons referred to in paragraphs (a) to (ac) (new paragraph (ad)).

411. The amendment to section 2(3) of the FOIA by which the exemptions in the new paragraphs (a) to (ab) are absolute, and those in the new paragraphs (ac) and (ad) are qualified (as they are subject to a public interest test), applies to Northern Ireland bodies.

412. The amendments made by the Constitutional Reform and Governance Act 2010 to sections 62(1) and 63 of the FOIA relating to historical records will also apply to Northern Ireland bodies. The amended section 62(1) provides for a change in the meaning of "historical record" so that a record becomes an "historical record" at 20 years rather than 30 years as previously.

413. The amended section 63 of the FOIA limits the exemptions from disclosure which can be applied to "historical records" so the maximum period for which information can be withheld is reduced from 30 years to 20 years for:

- sections 30(1) (investigations and proceedings conducted by public authorities), 32 (court records), 33 (audit functions), 35 (formulation of government policy) and 42 (legal professional privilege); and
- section 36 (prejudice to the effective conduct of public affairs), except for subsection (2)(a)(ii) (information which would or would be likely to prejudice the work of the Executive Committee of the Northern Ireland Assembly) and section 36(2)(c), in so far as disclosure would prejudice the effective conduct of public affairs in Northern Ireland where the lifespan of the exception remains at 30 years.

414. The amended section 63 also specifies the time limit applying to subsections 37(1)(a) to (ad) (communications with Her Majesty, etc). The time limit is 20 years after the creation of the record in which the information is contained, or five years after the death of the relevant member of the Royal Family, whichever is longer. In the case of communications with the Royal Household falling within new paragraph (ad), the relevant member of the Royal Family for these purposes is the Sovereign reigning when the record in question was created.

415. The maximum duration remains 30 years for sections 28 (relations within the UK) and 43 (commercial interests) of the FOIA.

416. *Subsection (2)* ensures that the power in section 46(2) to (5) of the Constitutional Reform and Governance Act 2010 may apply to Northern Ireland bodies. Subsections 46(2) to (5) of the Constitutional Reform and Governance Act 2010 allow transitional provisions to be made in connection with the amendments to the FOIA that reduce from 30 to 20 years the period within which certain exemptions from disclosure apply; give the Secretary of State power, by order, to make transitional arrangements relating to those amendments; enable provision to be made in any such order about the time when the exemptions cease to apply; and enable different provision to be made for records of different descriptions. A statutory instrument containing such an order is subject to the negative resolution procedure.

Section 105: Appointment and tenure of Information Commissioner

417. Section 105 makes further provision about the appointment and tenure of the Information Commissioner.

418. *Subsection (1)* amends paragraph 2(1) of Schedule 5 to the Data Protection Act 1998 ("DPA") with the effect that the Information Commissioner is appointed for a term not exceeding seven years. Currently the Commissioner is appointed for terms not exceeding five years.

419. *Subsection (2)* inserts new sub-paragraphs (3A) to (3C) into paragraph 2 of Schedule 5 to the DPA. Under paragraph 2(3) of Schedule 5 the Commissioner may be removed from office by Her Majesty in pursuance of an Address from both Houses of Parliament. New sub-paragraph (3A) sets out grounds for removing the Information Commissioner from his post. It also provides that an Address cannot be sought unless a Minister is satisfied that at least one of the listed grounds is met and presents a report to this effect.

420. New sub-paragraph (3B) provides that the Information Commissioner must be appointed on merit and on the basis of fair and open competition.

421. New sub-paragraph (3C) provides that the Information Commissioner may only serve a single term of office, and cannot be reappointed. As a consequence, subsection (2) repeals paragraph 2(5) of Schedule 5 to the DPA which currently permits reappointment of the Commissioner. This subsection also repeals paragraph 2(4) of Schedule 5 which requires the Commissioner to vacate his or her office on reaching 65 years of age.

422. *Subsection (4)* makes a consequential amendment to the heading of paragraph 2 of Schedule 5 to the DPA ('tenure of office' becomes 'tenure of office and appointment') to reflect the wider scope of this provision.

423. *Subsection (5)* repeals spent transitional provisions in section 18 of the FOIA in respect of the tenure of office of the Data Protection Commissioner following the change of name of that office to that of Information Commissioner.

Section 106: Alteration of role of Secretary of State in relation to guidance powers

424. Section 106 removes the current requirement that guidance issued by the Information Commissioner under sections 41C, 52A and 55C of the DPA relating to assessment notices, data sharing and monetary penalty notices respectively must be approved by the Secretary of State.

425. *Subsection (1)* replaces the current section 41C(7) of the DPA so as to require the Information Commissioner to consult the Secretary of State before issuing or amending a code of practice relating to assessment notices issued under section 41C. The current requirement for Secretary of State approval is removed.

426. *Subsection (2)* replaces the current section 52B(1) to (3) and amends section 52B(6) of the DPA to require the Information Commissioner to consult the Secretary of State when preparing a code of practice relating to data sharing under section 52A. The current requirement for Secretary of State approval, which can only be withheld where it appears that the terms of the code could result in the UK being in breach of its EU or other international obligations, is removed. A code of practice issued under section 52A must still be laid before Parliament by the Secretary of State.

427. *Subsection (3)* replaces the current section 55C(5) of the DPA to require the Information Commissioner to consult the Secretary of State before issuing a code of practice relating to his functions under sections 55A and 55B in respect of civil monetary penalties. The current requirement for Secretary of State approval is removed.

Section 107: Removal of Secretary of State consent for fee-charging powers etc.

428. Section 107 removes the current requirement in section 51(8) of the DPA and 47(4) of the Freedom of Information Act ("FOIA") for the Information Commissioner to obtain the consent of the Secretary of State before charging for services provided under section 51 of the DPA and section 47 of the FOIA.

429. *Subsections (1)* and *(3)* amend section 51 of the DPA and section 47 of the FOIA respectively to specify the relevant services for which the Information Commissioner can charge under those Acts, namely the supply of multiple copies of publications (that is, those that are reasonably accessible to the public free of charge because for example they can be downloaded from the Information Commissioner's Office ("ICO") website), and the provision of training and conferences. It does not permit the Commissioner to charge for his or her attendance (or that of his or her staff) at conferences organised by others. In each case the definition of "relevant services" may be amended by order made by the Secretary of State (by virtue of the amendments made to the DPA and the FOIA by *subsections (2)* and *(4)* such orders are subject to the negative resolution procedure).

Section 108: Removal of Secretary of State approval for staff numbers, terms etc.

430. Section 108 makes further provision about the appointment of staff by the Commissioner, and their terms and conditions.

431. *Subsection (1)* amends paragraph 4 of Schedule 5 to the DPA as set out in *subsections (2)* and *(3)*.

432. Subsection (2) inserts a new sub-paragraph (4A) into paragraph 4 of Schedule 5 of the DPA. This provides that when appointing a deputy commissioner or any other officers or staff, the Information Commissioner must have regard to the principle of selection on merit on the basis of fair and open competition.

433. Subsection (3) removes the existing requirement, in paragraph 4(5) of Schedule 5 to the DPA, on the Information Commissioner to obtain the Secretary of State's approval for the number of staff to be appointed to the ICO and to the terms and conditions of appointment of such staff.

Part 7: Miscellaneous and general

Section 109: Trafficking people for sexual exploitation

434. Section 109 inserts a new section 59A into the Sexual Offences Act 2003 ("the 2003 Act") to replace, expand and combine into one single integrated offence, the three separate trafficking offences in sections 57 to 59 of the 2003 Act, which made it an offence to traffick into, within or out of the UK for the purposes of sexual exploitation.

435. Subsection (1) of new section 59A makes it a criminal offence to intentionally arrange or facilitate the arrival in or entry into ((1)(a)), travel within ((1)(b)), or departure from ((1)(c)) the UK or any other country of another person for the purposes of sexual exploitation.

436. New section 59A(2) provides that the arranging or facilitating is done with a view to the sexual exploitation of B if A intends to do anything to or in respect of B, or believes that any other person is likely to do something to or in respect of B, after B's arrival, entry or departure from the UK which, if done, will involve the commission of a relevant offence. New section 59A(3) makes equivalent provision for the meaning of sexual exploitation where B is trafficked within the UK but here the exploitation may take place during or after the journey.

437. New section 59A(4) provides that a UK national commits an offence under section 59A regardless of where in the world the arranging or facilitating takes place or regardless of which country is the country of arrival, entry, travel or departure; new section 59A(5) provides that a non-UK national commits the offence if any part of the arranging or facilitating takes place in the UK or if the UK is the country of arrival, entry, travel or departure.

438. New section 59A(6) provides that a person found guilty under new section 59A will, on summary conviction, be liable to a term of imprisonment not exceeding 12 months

or a fine not exceeding the statutory maximum (or both). On conviction on indictment, a person is liable to a term of imprisonment not exceeding 14 years.

439. *Subsection (3)* substitutes a new subsection (1) into section 60 of the 2003 Act, which provides the relevant definitions for new section 59A and *subsection (5)* amends, consequently, the title of section 60. *Subsection (4)* repeals section 60(2) which provided for extra-territorial jurisdiction in respect of sections 57 to 59 of the 2003 Act.

Section 110: Trafficking people for labour or other exploitation

440. Section 110 amends the Asylum and Immigration (Treatment of Claimants, etc) Act 2004 ("the 2004 Act").

441. *Subsection (2)* inserts new subsections (1A) to (1C) into section 4 of the 2004 Act in place of subsections (1) to (3). New subsection (1A) makes it a criminal offence to intentionally arrange or facilitate the arrival in or entry into ((1)(a)), travel within ((1)(b)), or departure from ((1)(c)) the UK or any other country of another person for exploitation.

442. New subsection (1B) provides that the arranging and facilitating is done with a view to the exploitation of B if A intends to exploit B, or believes that any other person is likely to exploit B, after B's arrival, entry or departure from the UK or any part of the world.

443. New subsection (1C) makes equivalent provision for the meaning of exploitation where a person is trafficked within the UK, but here the exploitation may take place during or after the journey.

444. *Subsection (4)* inserts a new subsection (4A) in section 4 of the 2004 Act which provides that a UK national commits an offence under new subsection (1A) regardless of where in the world the arranging or facilitating takes place or which country is the country of arrival, entry, travel or departure; new subsection 4(4B) provides that a non-UK national commits the offence if any part of the arranging or facilitating takes place in the UK or the UK is the country of arrival, entry, travel or departure.

445. *Subsection (6)* provides the relevant definitions for the purposes of section 4.

Section 111: Offences in relation to stalking

446. *Subsection (1)* inserts a new section 2A into the Protection from Harassment Act 1997 which introduces a new offence of stalking. A person will be guilty of committing this new offence if that person pursues a course of conduct in breach of the prohibition on harassment in section 1(1) of the Protection from Harassment Act 1997 and the course of conduct amounts to stalking.

447. New section 2A(2) provides that a course of conduct amounts to stalking if it amounts to harassment, the acts or omissions involved are ones associated with stalking and the person knows or ought to know that the course of conduct amounts to harassment of the other person.

448. New section 2A (3) provides a non-exhaustive list of examples of behaviour that are associated with stalking, such as 'following a person' and 'watching or spying on a person'. This list of behaviours is based on some of those set out in section 39 of the Criminal Justice and Licensing Act (Scotland) Act 2010.

449. New section 2A(4) provides that this is a summary only offence with a maximum penalty of six months imprisonment or a fine not exceeding level 5 on the standard scale, or both.

450. *Subsection (2)* inserts new section 4A into the Protection from Harassment Act 1997 which introduces a new offence of stalking involving fear of violence or serious alarm or distress. A person would be guilty of the new offence where that person pursues a course of conduct amounting to stalking which causes another to fear, on at least two

occasions, that violence will be used against them or it causes the victim serious alarm or distress that has a substantial adverse effect on their usual day-to-day activities and the person knows or ought to know that his course of conduct will have such an effect on the victim.

451. New sections 4A(2) and 4A(3) provide that a person ought to know that his or her conduct will cause the other person to fear that violence will be used against them (new section 4A(2)) or will cause the other person serious alarm or distress (new section 4A(3)), if a reasonable person in possession of the same information would think it so. New section 4A(4) provides defences including, for example, if the person can show that his or her conduct was for the purpose of preventing or detecting crime.

452. New section 4A(5) provides that the offence will be an either way offence with a maximum penalty of five years imprisonment or an unlimited fine, or both, if tried in the Crown Court, or a fine up to £5000 or a term of imprisonment up to six months, or both, if tried in the magistrates' court.

Section 112: Power of entry in relation to stalking

453. Section 112 inserts a new section 2B into the Protection from Harassment Act 1997, which introduces a new power of entry in respect of the offence of stalking introduced by the new section 2A of the Protection from Harassment Act 1997 (inserted by section 111 of this Act). The new power of entry is exercisable by warrant to allow the police to enter and search premises if there are reasonable grounds for believing that an offence under new section 2A has been or is being committed and the other conditions in subsection (1) are met. New section 2B(2) provides that a constable may seize and retain anything for which the search has been authorised under section 2B(1).

Section 113: Repeal of provisions for conducting certain fraud cases without jury

454. Section 107 repeals section 43 of the Criminal Justice Act 2003, which makes provision in certain serious fraud cases for the prosecution to apply to the trial judge for the trial to be conducted without a jury. Section 43 has not been commenced.

Section 114: Removal of restrictions on times for marriage or civil partnership

455. This section repeals section 4 of the Marriage Act 1949 and provisions in section 17(2) of the Civil Partnership Act 2004 which limit the time during which a marriage or civil partnership can take place to between the hours of 8am and 6pm (subsections (1)(a) and (3)). The section also removes the associated offences in section 16(4) of the Marriage Act 1949 and section 31(2)(ab) of the Civil Partnership Act 2004 if a marriage or civil partnership takes place outside of these times (subsections (1)(b) and (4)). The effect of the section is to allow a marriage or civil partnership to take place at any time of the day or night.

456. *Subsection (2)* makes a consequential amendment to section 16(4) of the Marriage (Registrar General's Licence) Act 1970 which disapplied the offence in section 16(4) of the Marriage Act 1949 to a marriage solemnised on the authority of the Registrar General's licence.

Section 115: Consequential amendments, repeals and revocations

457. *Subsections (1)* and *(2)* introduce Schedules 9 and 10 to the Act which make consequential amendments and list repeals and revocations respectively.

458. *Subsection (3)* enables the Secretary of State, by order, to make further consequential amendments, including repeals and revocations. Where such an order does not amend primary legislation it is subject to the negative resolution procedure (*subsection (6)*), otherwise the affirmative resolution procedure applies (*subsection (5)*).

Schedule 9: Consequential amendments

Part 1: Destruction, retention and use of fingerprints and samples etc.

459. *Paragraph 3* makes amendments to the Police and Criminal Evidence Act 1984 ("PACE") to the powers to take DNA and fingerprints, consequential on the new retention regime set out in Chapter 1 of Part 1 of the Act. *Paragraph 4* repeals the uncommenced biometric retention provisions in sections 14, 16 to 19 and21 to 23 of the Crime and Security Act 2010.

Part 3: Safeguards for certain surveillance under RIPA

460. *Paragraphs 10* and *11*amend sections 57 and 62 of Regulation of Investigatory Powers Act 2000 ("RIPA") so as to provide that it is not part of the functions of the Interception of Communications Commissioner or the Chief Surveillance Commissioner to review the decisions of the relevant judicial authority to approve or reject authorisations or notices made by local authorities.

461. *Paragraph 12* allows the Investigatory Powers Tribunal to continue to consider complaints about the conduct by public authorities notwithstanding that the conduct has been approved by a relevant judicial authority.

462. *Paragraph 13* extends the powers of the Investigatory Powers Tribunal so that it may quash an order made by a relevant judicial authority under new section 23A or 32A of RIPA.

463. *Paragraph 14* amends section 71 of PACE so that the requirement on the Secretary of State to produce one or more codes of practice in respect of the exercise of the powers under the Act does not extend to the exercise of powers by the relevant judicial authority under new sections 23A or 32A of RIPA.

464. *Paragraph 15* amends RIPA to make provision in respect of the procedure which is to apply to applications to the sheriff for an order under new section 23A or 32A by specifying matters which must be secured by rules of court. These requirements are to ensure that the rules governing applications for judicial approval in Scotland will preserve the covert nature of the authorisation, notice or renewal while maintaining the power of the Court of Session to regulate and prescribe the procedure and practice to be followed in any civil proceedings in the sheriff court.

465. *Paragraphs 15* and*16* also amend RIPA to enable the Lord Chancellor, by order, to make procedural rules for district judges (magistrates' courts) in Northern Ireland in relation to local authority authorisations and notices for the acquisition of communications data and authorisations for covert human intelligence sources and directed surveillance. Currently, the Lord Chancellor has powers in relation to the making of Magistrate's Courts Rules in Northern Ireland which deal with excepted matters only. The court rules in relation to the new sections 23A and 32A of RIPA will need to deal with both reserved and excepted matters. As such, the order making power at new section 77B of RIPA allows the Lord Chancellor to make rules. New section 77B also provides that where the Magistrate's Courts Rules Committee (the body which makes rules for magistrate's courts in Northern Ireland) regulates and prescribes the procedure and practice to be followed in relation to an application to the district judge under new section 23A or 32A of RIPA, it is subject to, but not otherwise constrained by, the provisions relating to the judicial approval procedure in new sections 23B and 32B and any order made under new section 77B. Accordingly, if the Magistrates' Courts Rules Committee makes new court rules for the judicial approval process, it may not make provision which is contrary to that which is made by the Lord Chancellor in an order under new section 77B.

466. *Paragraph 17* inserts a new subsection (9) into section 81 (general interpretation) of RIPA to provide that the Secretary of State may make certain orders in respect of a

transferred matter in respect of Northern Ireland where that matter is ancillary to a reserved or an excepted matter.

Part 4: Vehicles left on land

467. *Paragraph 20* makes amendments to the Private Security Industry Act 2001 ("the 2001 Act") consequential upon section 54 which makes it an offence to immobilise, remove or restrict the movement of a vehicle without lawful authority. The 2001 Act provides for the licensing, by the Security Industry Authority ("SIA"), of individuals engaged in the immobilisation (wheel clamping) of vehicles. Sections 42 and 44 of the Crime and Security Act ("the 2010 Act") amended the 2001 Act so as to provide for the licensing of wheel clamping businesses and for an independent avenue of appeal for motorists in respect of release fees imposed by businesses carrying out wheel clamping and related activities; the provisions in the 2010 Act have not been brought into force. With the introduction of the new offence, the existing licensing regime becomes redundant, accordingly this paragraph repeals the relevant provisions of the 2001 Act, as amended, which provide for the licensing of wheel clamping operatives and companies.

Part 7: Criminal records

468. *Paragraph 109* extends the power of the Criminal Records Bureau ("CRB") to require an applicant for a criminal record certificate or an enhanced criminal record certificate to provide their fingerprints where there is a dispute about that person's identity in relation to the new up-date arrangements (provided for under section 83 of this Act).

469. *Paragraph 110* amends the Police Act 1997 ("the 1997 Act") to ensure that the CRB can access barred list information for the purposes of providing up-date information on criminal record and enhanced criminal record certificates under section 83 (of this Act).

470. *Paragraph 111* extends the functions of the independent monitor (appointed under section 119B of the 1997 Act) to review the disclosure of non-conviction information in an enhanced criminal record certificate, so that the independent monitor can also sample cases in which chief police officers provide or do not provide non-conviction information for the purposes of the up-dating arrangements.

471. *Paragraph 114* omits section 122(3A)(a) of the 1997 Act which enables the Secretary of State to refuse to issue a criminal record certificate or an enhanced criminal record certificate where the registered body that countersigned the application for the certificate has failed to comply with the code of practice issued under section 122(1) (such a code provides guidance to registered bodies on the discharge of their functions and on the use of the information contained in a certificate). This provision is redundant as a result of section 79 which removes the requirement on the Secretary of State to send a copy of a criminal record certificate or an enhanced criminal record certificate to the registered body which countersigned the application for a certificate.

Section 116: Transitional, transitory or saving provision

472. This section enables the Secretary of State by order to make transitional, transitory or saving provisions in connection with the coming into force of the provisions in the Act other than Chapter 1 of Part 1 (as to which, see section 25). Such an order is not subject to any parliamentary procedure.

Section 118: Channel Islands and Isle of Man

473. This section enables the provisions in Chapters 1 to 3 of Part 5 of the Act (which amend the Safeguarding Vulnerable Groups Act 2006 and Part 5 of the Police Act 1997) to be extended to the Channel Islands and Isle of Man by Order in Council; such an order is not subject to any parliamentary procedure.

Section 119: Extent

474. This section sets out the extent of the provisions of the Act, details of which are set out in paragraphs 74 to 82.

Section 120: Commencement

475. Section 120 provides for commencement, details of which are set out in the following paragraphs:

COMMENCEMENT

476. The following provisions of the Act come into force on Royal Assent:

- Sections 88 to 91 which make provision for the transfer of functions, property, rights or liabilities from the ISA and the CRB to the Disclosure and Barring Service;
- Section 113 (and associated provisions in Part 12 of Schedule 9 and Part 10 of Schedule 10) which repeals section 43 of the Criminal Justice Act 2003 which makes provision for certain fraud trials to be conducted without a jury; and
- in Part 7 (miscellaneous and general), sections 115(3) to (7) and 116 to 121.

477. The following provisions of the Act come into force two months after Royal Assent:

- section 39(2) and Schedule 2 (and associated provisions in Part 2 of Schedule 10) which repeal a number of powers of entry.

478. All other provisions will be brought into force by means of commencement orders made by the Secretary of State or, in the case of certain provisions relating to Wales in Chapter 2 of Part 1 (protection of biometric information on children in schools); Chapter 1 of Part 3 (powers of entry); and section 56 and Schedule 4 (keeper liability for certain parking charges), by the Welsh Ministers.

HANSARD REFERENCES

479. The following table sets out the dates and Hansard references for each stage of this Act's passage through Parliament.

Stage	*Date*	*Hansard Reference*
House of Commons		
Introduction	11 February 2011	Vol. 523 Col. 598
Second Reading	1 March 2011	Vol. 524 Col. 205-271
Committee	22 March 2011 24 March 2011 29 March 2011 5 April 2011 26 April 2011 28 April 2011 3 May 2011 10 May 2011 12 May 2011 17 May 2011	Hansard Protection of Freedoms Bill Public Bill Committee
Report and Third Reading	10 October 2011	Vol. 533 Col. 80-152
	11 October 2011	Vol. 533 Col. 201-300
Commons consideration of Lords Amendments	19 March 2012	Vol. 542 Col. 527-589

Stage	*Date*	*Hansard Reference*
House of Lords		
Introduction	12 October 2011	Vol. 730 Col. 1732
Second Reading	8 November 2011	Vol. 732 Col. 167-228
Committee	29 November 2011	Vol. 733 Col. 131-232
	6 December 2011	Vol. 733 Col. 622-685
	13 December 2011	Vol. 733 Col. GC277-GC330
	15 December 2011	Vol. 733 Col. GC351-GC392
	12 January 2012	Vol. 734 Col. GC1-GC74
Report and Third Reading	31 January 2012	Vol. 734 Col. 1500-1556
	6 February 2012	Vol. 735 Col. 11-35,47-86,107-120
	15 February 2012	Vol. 735 Col. 791-864
Lords consideration of Commons Reason and Amendments	24 April 2012	Vol. 736 Col. 1714-1745
Royal Assent	1 May 2012	Vol. 736 Col. 2114 (Lords)
		Vol. 543 Col. 1371 (Commons)

ANNEX A: GLOSSARY

1956 Act	Sexual Offences Act 1956
1984 Act	Data Protection Act 1984
1994 Act	Public Order Act 1994
1997 Act	Police Act 1997
2000 Act	Terrorism Act 2000
2001 Act	Private Security Industry Act 2001
2003 Act	Criminal Justice Act 2003
2004 Act	Asylum and Immigration (Treatment of Claimants, etc.) Act 2004
2008 Act	Counter-Terrorism Act 2008
2009 Act	Policing and Crime Act 2009
2010 Act	Crime and Security Act 2010
ANPR	Automatic Number Plate Recognition
CCTV	Closed Circuit Television
CHIS	Covert Human Intelligence Source
CRB	Criminal Records Bureau
DBS	Disclosure and Barring Service
DPA	Data Protection Act 1998
DVLA	Driver and Vehicle Licensing Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FOIA	Freedom of Information Act 2000
ICC	International Criminal Court
ICO	Information Commissioner's Office
ISA	Independent Safeguarding Authority
PACE	Police and Criminal Evidence Act 1984
PNC	Police National Computer
RIPA	Regulation of Investigatory Powers Act 2000
SIA	Security Industry Authority
SRSA 2007	Statistics and Registration Service Act 2007
SVGA	Safeguarding Vulnerable Groups Act 2006
SVGO	Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
TPIM	Terrorism Prevention and Investigation Measure

ANNEX B:

DNA Profile Retention Periods: Comparison between current rules under PACE, the rules applicable in Scotland, and the rules that would apply under the provisions in the 2010 Act and in Chapter 1 of Part 1 of this Act

Occurrence	*Current System (E&W)*	*Crime & Security Act 2010 – E&W*	*Scottish System*	*Changes under this Act*
ADULT – Conviction – All Crimes	Indefinite	Indefinite	Indefinite	Indefinite
ADULT – Charged but not Convicted – Serious Crime	Indefinite[1]	6 Years	3 Years + possible 2-year extension(s) by Court	3 Years + possible single 2-Year extension by Court
ADULT – Arrested but not Charged or Convicted – Serious Crime	Indefinite[1]	6 Years	None	Only where authorised by the Commissioner – 3 Years + possible single 2-year extension by Court
ADULT – Non Conviction – Minor Crime	Indefinite[1]	6 Years	None	None[1]
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 – Charged but	Indefinite[1]	3 Years	3 Years + possible 2-year	3 Years + possible single 2-

*
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.

§
On the basis of arrest – no specific provision for PNDs.

1
1
1
1
1

Occurrence	*Current System (E&W)*	*Crime & Security Act 2010 – E&W*	*Scottish System*	*Changes under this Act*
not Convicted – Serious Crime			extension(s) by Court	Year extension by Court
UNDER 18s – Arrested but not Charged or Convicted – Serious Crime	Indefinite[1]	3 Years	None	Only where authorised by the Commissioner – 3 Years + possible single 2-year extension by Court
UNDER 18s – Non Conviction – Minor Crime	Indefinite[1]	3 Years	None	None[1]
Penalty Notice for Disorder	Indefinite[1]	6 Years[1]	2 Years	2 Years
Terrorist suspects	Indefinite[1]	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 (Commissioner will review all determinations)
Biological DNA Samples	Indefinite[1]	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.				
§ On the basis of arrest – no specific provision for PNDs.				

1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1

1