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

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 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

1 http://webarchive.nationalarchives.gov.uk/20100526084809/http://programmeforgovernment.hmg.gov.uk
2 http://www.bailii.org/eu/cases/ECHR/2008/1581.html

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 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*

---

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

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 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).

---

7 http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/review-findings-and-rec?view=Binary

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 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;

---

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
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

- 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.

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

---

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

14 http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/counter-terrorism-statistics/hosb0412/hosb0412?view=Binary

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 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

---

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/
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.

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.

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

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

22 http://www.homeoffice.gov.uk/publications/legislation/protection-freedoms-bill/

- 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);
- 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

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 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.

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

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

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).