



# **Memorandum to the Home Affairs Committee**

## **Post-Legislative Scrutiny of the Protection of Freedoms Act 2012**

Presented to Parliament  
by the Secretary of State for the Home Department  
by Command of Her Majesty

March 2018

Cm 9579



# **Memorandum to the Home Affairs Committee**

## **Post-Legislative Scrutiny of the Protection of Freedoms Act 2012**

Presented to Parliament  
by the Secretary of State for the Home Department  
by Command of Her Majesty

March 2018

Cm 9579



© Crown copyright 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3)

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications>

Any enquiries regarding this publication should be sent to us at:

Finance and Planning Unit  
Home Office  
2 Marsham Street SW1P 4DF

[CPFGBusinessSupportTeam@homeoffice.gsi.gov.uk](mailto:CPFGBusinessSupportTeam@homeoffice.gsi.gov.uk)

ISBN 978-1-5286-0235-8

CCS0218087168

03/18

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

## **MEMORANDUM TO THE HOME AFFAIRS SELECT COMMITTEE**

### **POST-LEGISLATIVE ASSESSMENT OF THE PROTECTION OF FREEDOMS**

#### **ACT 2012**

#### **INTRODUCTION**

1. The memorandum provides a preliminary assessment of the Protection Of Freedoms Act 2012 (2012 c 09) and has been prepared by the Home Office for submission to the Home Affairs Committee. It is published as part of the process set out in the document Post Legislative Scrutiny – The Government’s Approach (Cm 7320).

#### **OBJECTIVES OF THE PROTECTION OF FREEDOMS ACT 2012**

2. The Protection of Freedoms Act is an Act (PoFA) that: provides for the destruction, retention, use and other regulation of certain evidential material; imposes consent and other requirements in relation to certain processing of biometric information relating to children; provides for a code of practice about surveillance camera systems and for the appointment and role of the Surveillance Camera Commissioner; provides for judicial approval in relation to certain authorisations and notices under the Regulation of Investigatory Powers Act 2000; provides for the repeal or rewriting of powers of entry and associated powers and for codes of practice and other safeguards in relation to such powers; makes provision about vehicles left on land; amends the maximum detention period for terrorist suspects; replaces certain stop and search powers and to provide for a related code of practice; makes provision about the safeguarding of vulnerable groups and about criminal records including provision for the establishment of the Disclosure and Barring Service and the dissolution of the Independent Safeguarding Authority; disregards convictions and cautions for certain abolished offences; makes provision about the release and publication of datasets held by public authorities and makes other provision about freedom of information and the Information Commissioner; makes provision about the trafficking of people for exploitation and about stalking; repeals certain enactments; and provides for connected purposes.
3. As the Protection of Freedoms Act is split into seven parts and also covers powers associated with government departments other than the Home Office, we have taken the decision to handle the PLS memo in the following manner. This note deals with each part of the Act as a separate entity and provides post legislative scrutiny information for each set of related powers as set out in table 1:

<b>PROVISION</b>	<b>PAGE</b>
Part 1- Regulation of biometric data – Chapter 1, Destruction, retention and use of fingerprints etc	5
Part 1 – Regulation of biometric data – Chapter 2, Protection of Biometric Information in Schools	22
Part 2 - Regulation of surveillance – Chapter 1, Regulation of (CCTV) & Automatic Number Plate Recognition (“ANPR”)	25
Part 2 - Regulation of surveillance - Safeguards for RIPA surveillance	29
Part 3 - Protection of property from disproportionate enforcement action – Chapter 1, repealing and amending powers of entry; codes concerning use of powers	32
Part 3 - Protection of property from disproportionate enforcement action – Chapter 2, offence concerning vehicles left on land; power to remove vehicles; recovery of unpaid parking charges	37
Part 4 - Counter-terrorism powers - Amends Schedule 8 Terrorism Act re maximum detention period; repeals and replaces stop and search powers	40
Part 5 -Safeguarding vulnerable Groups – Chapter 1, changes to Safeguarding of Vulnerable Groups Act 2006 (“SVGA” & corresponding amendments in NI	47
Part 5 -Safeguarding vulnerable Groups – Chapter 2, changes to criminal records	54
Part 5 -Safeguarding vulnerable Groups – Chapter 3, Disclosure and barring service	60
Part 5 -Safeguarding vulnerable Groups – Chapter 4, disregarding certain convictions for buggery	67
Part 6 – Freedom of Information and Data Protection - amendments to FOIA and DPA	75
Part 7 - Miscellaneous and General - trafficking people for exploitation <b>REPEALED</b>	77
Part 7 - Miscellaneous and General - offences and powers of entry in relation to stalking	79
Part 7 - Miscellaneous and General - repeal of fraud cases being heard without a jury	85
Part 7 - Miscellaneous and General - removal of time limitations for marriage and civil ceremonies	86

**Table 1: organisation of this post legislative scrutiny note**

## **PART 1 – REGULATION OF BIOMETRIC DATA**

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

Introduction:

1. Chapter 1 of Part 1 made 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 replaced 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 could 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).
2. The police can also 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 was 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. This change in regime resulted from the European Court of Human Rights (“ECtHR”) decision in the case of *S and Marper v the United Kingdom* in December 2008, [2008] ECHR 1581. The ECtHR ruled that the provisions in PACE (and the equivalent legislation in Northern Ireland) permitting the ‘blanket and indiscriminate’ retention of DNA from un-convicted individuals violated Article 8 (right to privacy) of the European Convention on Human Rights (“ECHR”).
3. In response to this judgment, the then Government brought forward provisions in 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 & 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 were not brought into force because the Coalition Government felt that the retention periods it set out were too long and Part 1 of Schedule 10 of the Act repealed them (save for sections 15 & 20). Police powers in Scotland in this area are contained in sections 18 to 20 of the Criminal Procedure (Scotland) Act 1995 (as amended).

4. The Programme for Government (section 3: civil liberties) published by the then Coalition Government in 2010 stated that it would “*adopt the protections of the Scottish model for the DNA database*”. The Act introduced a new model for destruction and retention of DNA samples, DNA profiles and fingerprints into effect in England and Wales, and in relation to national security cases in Northern Ireland, which was, in broad terms, modelled on the regime which applies in Scotland.
5. The Act requires that a DNA sample is destroyed once a DNA profile has been derived from it, or after six months; whichever is the earlier. A DNA profile is a sequence of numbers representing a small part of the person’s DNA, which is sufficient for very accurate unique identification. A sample could potentially be used to produce information on any of a person’s inherited characteristics; this measure is designed to prevent this. This provision is subject to the retention of samples for the purposes of the Criminal Procedure and Investigations Act (see ‘legal issues’ section below for further details).
6. Under the regime set out in this Chapter, the fingerprints and DNA profiles taken from individuals arrested for or charged with a minor<sup>1</sup> offence are destroyed following either a decision not to charge or acquittal (unless they have a previous conviction for a recordable offence, in which case it may be retained indefinitely). In the case of those charged with, but not convicted of, a serious offence, their fingerprints and DNA profile 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’ Court) where this is necessary to assist in the prevention or detection of crime.

---

<sup>1</sup> Minor offences are non-qualifying offences.

7. In the case of those arrested under the Terrorism Act 2000, their fingerprints and DNA may be retained for three years (or indefinitely if they are convicted of a recordable offence), and in the case of those examined under Schedule 7 to the Terrorism Act 2000 their biometrics may be retained for six months. In any case, chief officers of police may make a 'national security determination' authorising further retention for a (renewable) period of two years, subject to review and approval by the Biometrics Commissioner.
  
8. The Protection of Freedoms Act also creates the post of Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner') who is appointed by the Home Secretary. The Commissioner has three main functions:
  - to oversee police use of DNA and fingerprints taken under PACE and counter-terrorism legislation;
  - to keep under review 'National Security Determinations' (NSDs) made or renewed by the police allowing retention of an individual's biometric material beyond the period otherwise permitted for the purposes of national security;
  - to consider applications from the police to retain DNA and fingerprints taken under PACE from individuals arrested for, but not charged with, a qualifying<sup>2</sup> offence. Where he agrees to allow retention, they may be retained for a period of three years (with a single two-year extension available on application by a chief officer of police to a District Judge (Magistrates' Court)).
  
9. The Biometrics Commissioner is also required to make an annual report to the Home Secretary about the carrying out of these functions.
  
10. Where an individual is convicted of a recordable<sup>3</sup> offence, their DNA and fingerprints may be retained indefinitely. Where they receive a Penalty Notice for Disorder it may be retained for a period of two years.

---

<sup>2</sup> 'Qualifying' offences are more serious offences, largely sexual and violent offences, plus burglary. They are listed under section 65A of the Police and Criminal Evidence Act 1984.

<sup>3</sup> A 'recordable' offence is one for which the police are required to keep a record. Generally speaking, these are imprisonable offences; however, it also includes a number of non-imprisonable offences such as begging and taxi touting.



11. Where an individual aged under 18 is convicted of a first minor offence (i.e. a non-qualifying offence) and they receive a custodial sentence for a period of less than five years, their DNA and fingerprints are only retained for five years (plus the length of any custodial sentence they are convicted of). Where they receive a sentence of over five years custody then their biometric material may be retained indefinitely.
12. The Protection of Freedoms Act also makes provision for the governance and oversight of the police use of DNA and fingerprints. It requires the Home Secretary to establish a National DNA Strategy Board to oversee the operation of the National DNA Database.

### **IMPLEMENTATION:**

13. Section 20(1), (10) & (11) were brought into force on 1st October 2012 with the remaining sub-sections coming into force on 31st October 2013. Sections 1 - 12, 15 – 16, 20(2) - (9) & 21 - 25 came into force on 31st October 2013, with some exceptions relating to national security material held prior to that date ('legacy material'). These were as follows:
  - Section 1 came fully into force in relation to legacy material which required consideration under section 9 (retention for purposes of national security);
  - Section 19 (and Schedule 1 which has effect as a result of section 19) came fully into force in Great Britain in relation to legacy material taken, held or derived from a DNA sample taken under certain specified terrorism legislation, on 31<sup>st</sup> October 2016; and
  - Section 19 and Schedule 1 will come fully into force in Northern Ireland on 31<sup>st</sup> October 2018 in relation to the same category of legacy material.
  - Section 13 was partially brought into force on 31<sup>st</sup> October 2013 with the remaining sub-sections coming into force on 31<sup>st</sup> January 2014. Section 14 was partially brought into force on 31<sup>st</sup> October 2013.
14. The whole of Chapter 1 of Part 1 of the Protection of Freedoms Act was brought into force (subject to certain amendments) with the exception of section 19 in relation to Northern Ireland.
15. PSNI is compliant with the Protection of Freedoms Act for material taken post October 2013. Material taken before this is being retained by PSNI under the Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric

Data) (Transitional, Transitory and Saving Provisions) Order 2016. This transitional order was implemented in order to retain historic legacy material which might be of investigative value to the work of the Historical Investigations Unit (HIU). The HIU is one of four planned new institutions which are part of a range of measures intended to implement the Stormont House Agreement in order to help Northern Ireland address the issues of the past. The HIU will have access to a snapshot of relevant fingerprints and DNA profiles, however the body itself has not been established yet. As part of the ongoing political talks process, the political parties are being consulted on possible forms for the new SHA institutions and the Secretary of State for Northern Ireland has confirmed his intention to carry out a public consultation on the proposed new institutions. In the interim, however, without an appropriate body to pass the biometric material to it has not been possible for the PSNI to fully commence the Protection of Freedoms Act regime. The transitional Order was therefore necessary to protect the relevant material from deletion until the HIU can be established. NIO officials are working closely with the PSNI and legal advisors to draft wording in the legislation establishing the HIU that will establish the parameters of the data that will form the 'snapshot'.

16. Secondary legislation associated with this part of the Protection of Freedoms Act was as follows in table 2:

<b>Section</b>	<b>Related SI</b>	<b>Purpose</b>	<b>Date of Issue<sup>4</sup></b>
25	<u>The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) Order 2013 (2013 No, 1813)</u>	Provided for the destruction or retention of legacy biometric material taken before the Protection of Freedoms Act came into force	17 <sup>th</sup> July 2013

<sup>4</sup> This is the date that the SI was signed by the Minister.

<b>Section</b>	<b>Related SI</b>	<b>Purpose</b>	<b>Date of Issue<sup>4</sup></b>
20/22	<u>The Protection of Freedoms Act 2012 (Commencement No.3) Order 2012 (2012 No. 2234)</u>	Required the Home Secretary to create the post of Commissioner for the Retention and Use of Biometric Material and established terms of office and guidance on the making of national security determinations. Note that this SI also commenced many other parts of the Protection of Freedoms Act outside Chapter 1 Part 1.	18 <sup>th</sup> July 2013
Part 1 Chapter 1 in general	<u>The Protection of Freedoms Act 2012 (Commencement No.7) Order 2013 (2013 No. 1814)</u>	Commenced Chapter 1 Part 1 of the Act (with the exception of section 20 (1), (10) and (11) and section 22) on the dates described in the 'implementation' section above	18 <sup>th</sup> July 2013
Part 1 Chapter 1 in general	<u>The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) (No.2) Order 2013 (2013 No. 2770)</u>	Amended Order 2013 No.1813 above to make provision in relation to an individual whose DNA profile or fingerprints were taken before 30 <sup>th</sup> September 2014. If such an individual was arrested for, or charged with, a subsequent offence, or was convicted or given a penalty notice for a subsequent offence, then it allowed their profile or fingerprints to be retained by the rules applicable to that subsequent offence.	28 <sup>th</sup> October 2013
22	<u>The Protection of Freedoms Act 2012 (Guidance on the Making or Renewing of National Security Determinations) Order 2014 (2014 No.198)</u>	Brought into force guidance published under section 22 of the Protection of Freedoms Act (see above)	3 <sup>rd</sup> February 2014
22	<u>The Protection of Freedoms Act 2012 (Destruction, Retention and Use</u>	Amended Order 2013 No.1813 above so that commencement was delayed by a year (from 31 <sup>st</sup>	30 <sup>th</sup> September 2015

Section	Related SI	Purpose	Date of Issue <sup>4</sup>
	<u>of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) Order 2015 (2015 No.1739)</u>	October 2015 to 31 <sup>st</sup> October 2016) of the requirement to delete material held or taken under certain specified terrorism legislation, or in relation to which consideration of a National Security Determination is required, which was first taken before 31 <sup>st</sup> October 2013.	
22	The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) Order 2016 (2016 No.682)	Amended Order 2013 No.1813 above, so that the requirement to delete material held or taken in Northern Ireland under certain specified terrorism legislation before 31 <sup>st</sup> October 2013 will not be commenced until 31 <sup>st</sup> October 2018.	27 <sup>th</sup> June 2016

**Table 2: Secondary legislation associated with this part of the Protection of Freedoms Act**

17. The following guidance was issued under Chapter 1, part 1 of the Protection of Freedoms Act, shown in table 3:

Section	Related Guidance	Purpose	Date of Issue <sup>5</sup>
22	<u>Guidance on the making or renewing of national security determinations allowing the retention of biometric data</u>	Provided guidance to any police force or other law enforcement agency about the making or renewing of a national security determination allowing the retention and use of biometric material for national security purposes	June 2013
24 (section 63(AB)(6) of PACE)	<u>Governance Rules for the National DNA Database Strategy Board</u>	Established the parameters under which the National DNA Database and Fingerprint Strategy Board operates	13 <sup>th</sup> June 2014
24 (section	<u>Applications to the</u>	Provided guidance to police	26 <sup>th</sup>

<sup>5</sup> This is the date that the guidance was published on gov.uk.

<b>Section</b>	<b>Related Guidance</b>	<b>Purpose</b>	<b>Date of Issue<sup>5</sup></b>
63(AB)(4) of PACE)	<u>Biometrics Commissioner under PACE</u>	forces on the circumstances under which they can apply to the Biometrics Commissioner for the retention of an individual's DNA and/or fingerprints when these would otherwise fall to be destroyed	September 2014
24 (section 63(AB)(2) of PACE)	<u>Deletion of Records from National Police Systems (PNC/NDNAD/IDE NT1)</u>	To provide guidance to police forces on the circumstances under which an individual can apply to have their fingerprints, DNA and/or Police National Computer records destroyed where these are held under a power set out under PACE.	27 <sup>th</sup> May 2015
1-16 (sections 63D-T of PACE)	<u>The NDNAD Strategy Board Policy for Access and Use of DNA Samples, Profiles and Associated Data</u>	To provide guidance to law enforcement agencies on the proper access to and use of DNA samples and profiles taken from suspects	31 <sup>st</sup> December 2015

**Table 3**

18. Following the commencement of Part 1 Chapter 1 of the Protection of Freedoms Act, it was realised that there were five issues which arose from the drafting. These were as follows:

- The power to take DNA and fingerprints if an investigation is restarted  
Previously, PACE stated that once a DNA sample had been taken from an arrested individual, a sample of the same type could not be taken again during the course of the same investigation unless the first sample proved insufficient. Therefore, if an investigation was stopped, the DNA sample was destroyed as required by the Act, and the investigation was later restarted, another sample could not be taken unless the individual consented to it. The problem was rectified by section 144 of the Anti-Social Behaviour Crime and Policing Act 2014 ("ASBCPA") which amended sections 61 & 63 of PACE to provide the police with the power to resample under these circumstances without consent.
- The power to retain fingerprints or DNA in connection with a different offence

Parliament's intention, when enacting the Protection of Freedoms Act, was that if a conviction in an individual's criminal history allows retention, then their DNA profile should be retained, regardless of whether the arrest for which the profile was obtained was itself followed by a conviction. However, the language in the Protection of Freedoms Act did not achieve this because it placed a requirement for a causal relationship between the sampling arrest and any conviction before a person's DNA profile could be held. It stated:

"...if section 63D material (DNA and fingerprints) which is taken from a person in connection with the investigation of an offence leads to the person to whom the material relates being arrested for, charged with or convicted of an offence".

This would have required some convicted offenders to have their DNA deleted from the National DNA Database where there was no relationship between the sampling arrest and the conviction. Section 145 of ASBCPA removed the requirement for the material taken on the sampling arrest to 'lead to' a later arrest, charge or conviction.

- The power to retain samples which are, or may become, disclosable under the Criminal Procedure and Investigations Act 1996 ("CPIA")

Section 14 of the Protection of Freedoms Act required DNA samples taken from individuals to be destroyed within six months of being taken. The great majority of samples taken for DNA analysis can safely be destroyed once a profile has been derived from them but some samples are needed as evidence and this destruction would prevent this. Section 146 of ASBCPA extended the regime set out under CPIA so that samples are treated in the same way as other forensic evidence needed for court purposes. Samples retained under the CPIA can only be used in relation to that particular offence and must be destroyed once their potential need for use as evidence has ended.

- Retention of DNA and fingerprints on the basis of convictions outside England and Wales.

Before April 2017, fingerprints and DNA profiles could only be retained indefinitely, in certain circumstances, if an individual with a previous conviction outside England and Wales (or outside the UK for fingerprints or DNA taken under the Terrorism Act 2000) was arrested under PACE for a recordable offence and no further action was taken in relation to the arrest offence, or if they were arrested under section 41 or detained under Schedule 7 to the Terrorism Act 2000. Under these circumstances, the law required that the individual be re-arrested and re-sampled, rather than the DNA profile and fingerprints already taken being retained. Furthermore, the power to retain applied only if the conviction was for an offence equivalent to a qualifying offence rather than for

the equivalent of any recordable offence as would be the case for a conviction in England and Wales. Before the passage of the Protection of Freedoms Act this had little practical effect as the DNA profile and fingerprints could (in broad terms) be retained because of the arrest, regardless of whether the person had any convictions. However, once Part 1 Chapter 1 of the Protection of Freedoms Act came into force this was no longer the case. Section 70 of the Policing and Crime Act 2017 amended the law to avoid the need for resampling and to allow retention of DNA profiles and fingerprints taken in England and Wales (or anywhere in the UK if taken under the Terrorism Act 2000) on the basis of the equivalent of recordable convictions elsewhere.

- Whether national security determinations should be made in relation to individuals or material

Following the conclusion of the police review of legacy national security material in October 2016 (see below), a potential drafting issue has been identified in relation to 'new material' (taken since 31st October 2013) in national security cases. Section 9 and Schedule 1 provide that a national security determination may be made by a police force in relation to 'material'. However in practice multiple sets of biometric material might be held in relation to the same one individual, if for example they have been arrested on more than one occasion. The Protection of Freedoms Act is currently being interpreted under these circumstances as requiring a separate national security determination to be made in relation to each set of material (and potentially by different police forces if the arrests occurred in different force areas), risking unnecessary complexity and duplication of effort, even though the necessity and proportionality case for each determination in relation to the same individual is likely to be identical. We are working with the police to consider this issue and whether any procedural changes or amendments to the Protection of Freedoms Act may be required. As stated above, the Biometrics Commissioner is required to produce an annual report on police use of DNA and fingerprints. The most recent annual report was published in March 2016 here:

<https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2014-to-2015>

The Government published a formal response in December 2016:

<https://www.gov.uk/government/publications/response-to-the-biometrics-commissioners-annual-report-2015>

And a further report on national security issues raised in the March 2016 annual report was published in May 2016:

<https://www.gov.uk/government/publications/biometrics-commissioners-annual-report-2015-further-report>

The Commissioner found in his annual report (at paragraph 251) that the 'overwhelming bulk' of DNA profiles and fingerprints had been retained or deleted in accordance with the legislation. The Commissioner's principal recommendations and the Government response were as follows:

- The list of qualifying offences (see above) should be reviewed and consideration given to inserting firearms and drugs offences. The government has stated that it will put forward amendments through a statutory instrument.
- The law should be changed to enhance powers to retain DNA and fingerprints taken in England and Wales on the basis of convictions in England and Wales. As stated above, this was done by the Policing and Crime Act 2017.
- Clearer guidance should be issued to forces on various technical issues relating to the use of the Police National Computer to implement the provisions of the Protection of Freedoms Act. Some guidance has been issued and further guidance is being prepared.

The Commissioner also highlighted in his annual report that handling and other delays had led to the statutory retention period expiring in some national security cases before a national security determination had been considered or sought, with the consequence that biometric records which might otherwise have been retained had to be deleted. In some of those cases the records were not then deleted when they should have been. At the Home Secretary's request the Commissioner prepared a further report on this issue which was published in May 2016, and which found that 'proper steps have been and are being taken to remedy the expiry and deletion problems..., to minimise the risk of their recurrence, and to mitigate their adverse consequences'.

### **Preliminary assessment of the Act:**

19. Overall, we believe that Chapter 1 of Part 1 of the Protection of Freedoms Act has generally been implemented successfully. This is evidenced by the Biometrics Commissioner's Annual Reports. However, there have been some issues arising from the drafting of the provisions which ideally should have been



addressed during the passage of the legislation; these are outlined above. Additionally, both the previous Biometrics Commissioner (in both his annual reports<sup>67</sup>) and the DNA Ethics Group (in its sixth annual report<sup>8</sup>) have expressed concern at the lack of research into the effectiveness of the Protection of Freedoms Act.

### **Destruction of fingerprints and DNA profiles (section 1)**

20. Amended PACE by inserting section 63D which defines the circumstances under which DNA must be destroyed.
21. This section has had the effect intended by Parliament of ensuring that fingerprints and DNA profiles taken or held by the police must be either retained on a clear statutory basis provided by the Protection of Freedoms Act or promptly destroyed.
22. The destruction of DNA profiles which did not meet the new retention criteria required considerable software changes to the Police National Computer and the national DNA and fingerprint databases. It was also not considered appropriate to immediately delete national security fingerprints and DNA profiles already held ('legacy material'), and commencement of the destruction requirement in relation to this material (both in section 1 and in Schedule 1 where it amended certain terrorism legislation) was delayed to allow such material to be reviewed and the necessity and proportionality of its continued retention considered by the Metropolitan Police Service (under section 19) during a transitional period. Although the Protection of Freedoms Act received Royal Assent in May 2012, for these reasons this section was not brought into effect until October 2013 in relation to general crime<sup>9</sup>, and October 2016 in relation to national security cases<sup>10</sup>.

### **Retention of fingerprints and DNA profiles (sections 2 – 8)**

23. Amended PACE by inserting sections 63E – L which defines the circumstances under which DNA may be retained.

---

<sup>6</sup><https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014>

<sup>7</sup><https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2014-to-2015>

<sup>8</sup> <https://www.gov.uk/government/publications/ndnad-ethics-group-6th-annual-report-2013>

<sup>9</sup> [The Protection of Freedoms Act 2012 \(Commencement No.7\) Order 2013 \(2013 No. 1814\)](#)

<sup>10</sup> [The Protection of Freedoms Act 2012 \(Destruction, Retention and Use of Biometric Data\) \(Transitional, Transitory and Saving Provisions\) \(Amendment\) Order 2016 \(2016 No.682\)](#)

24. The sections of the Protection of Freedoms Act relating to retention have generally worked well. They have ensured that the privacy of innocent people is safeguarded, whilst ensuring that the DNA and fingerprint databases continue to provide an important and effective tool for the police in solving crime and protecting the public from the threat of terrorism. Despite the deletion of 1.76 million profiles the match rate has continued to rise year on year (63.3% in 2015/16).
25. Although the indefinite retention of DNA profiles has been challenged in the domestic courts, the courts have found in the Government's favour.
26. A number of issues, mainly around the mechanics of recording in relation to the Police National Computer have been uncovered and these have yet to be fully resolved. The complexities of PNC coding led initially to some profiles being destroyed which did not need to be and, equally, some being retained unlawfully.
27. The need to de-link the DNA raw data from Forensic Service Providers (which renders the data unavailable to reconstitute a record, but does not completely delete the record) was quite costly to implement.
28. Some guidance for forces has been issued; a working group continues to consider these and will produce further guidance.

**Material retained for the purpose of national security (section 9)**

29. Amended PACE by inserting section 63M. This section, together with section 19 and Schedule 1 (see below), has ensured that police forces are able to retain biometric data where this is necessary for national security purposes. Guidance on making national security determinations has been issued under section 22. The requirement at section 20 that all national security determinations be reviewed by the Biometrics Commissioner, and the power for the Commissioner to order the deletion of material if he is not satisfied that its retention is necessary, provides an important and effective safeguard for the rights of individuals whose data is retained under these powers.
30. As well as reviewing individual cases, the Biometrics Commissioner is also responsible for overseeing the general process for making national security determinations. He has reported that it is generally working well and that the police are implementing the system in a 'sensible and proper manner', and that

‘Chief Officers...and their deputies have been giving careful consideration to [national security determination] applications before deciding whether or not to approve them’.

31. However the Commissioner’s 2015 report did identify some challenges in implementing the national security determination system, which gave rise to delays and other errors and resulted in the loss of some data which might otherwise have been retained on national security grounds (see above). In a subsequent report on these issues, published in May 2016, the Commissioner found that they were being satisfactorily addressed and steps taken to prevent their recurrence.

32. More generally, although the national security determination system has broadly been successfully implemented and has had the effect Parliament intended, the police have reported finding the process resource intensive and at times complex to manage. They have noted that a range of different retention periods may apply to a given national security case depending on its circumstances, and that in some cases the timescale for considering whether a national security determination is necessary can be challenging. We are working with the police to consider whether any procedural or other changes may support a more streamlined implementation of the system.

**Material given voluntarily and with consent (sections 10 & 11)**

33. Amended PACE by inserting sections 63N & O which set out what must happen to DNA and fingerprints given voluntarily. Forms for different types of retention of DNA have been drawn up including voluntary retention of sex offenders and the taking of samples from volunteers for elimination purposes for use in specific cases. And guidance has been issued on access (see above). We are not aware of any difficulties with the operation of this section of the Protection of Freedoms Act.

**Material obtained for one purpose and used for another (section 12)**

34. Amended PACE by inserting section 63P which sets out what must happen to material taken for one offence and used for another. Section 63P was amended by section 145 of ASBCPA (see above section on the power to retain fingerprints or DNA in connection with a different offence under Drafting Issues).

**Destruction of copies (section 13)**

35. Amended PACE by inserting section 63Q which extended any requirement to destroy DNA and fingerprints to any copies made. The destruction of hard copies of fingerprints proved particularly challenging for forces because they require manual review, whereas records held on the national fingerprint database are deleted automatically. As a result, this section was not brought in until January 2014.

#### **Destruction of samples (section 14)**

36. Amended PACE by inserting section 63R which defines the circumstances under which DNA samples must be destroyed. The destruction of samples which did not meet the requirements prior to commencement was achieved by May 2013; with the destruction of elimination samples being completed by June 2016.

#### **Destruction of Impressions of Footwear (section 15)**

37. Amended PACE by inserting section 63S which requires the destruction of footwear impressions which are no longer required. We are not aware of any current issues with the operation of this section of the Protection of Freedoms Act.

#### **Use of retained material (section 16)**

38. Amended PACE by inserting section 63T which restricts the use of material retained under the Protection of Freedoms Act to one of four circumstances:

- where its use is in the interests of national security,
- for the purposes of a terrorist investigation,
- for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution; or
- for purposes related to the identification of a deceased person or of the person to whom the material relates.

39. This section of the Protection of Freedoms Act was considered in the case of “R v Z” where it was argued that blood obtained from a crime scene (under part 2 of PACE) could be used for the purposes of paternity testing. The Family Division of the High Court ruled in favour of this interpretation but the Court of Appeal overturned the ruling, finding that DNA taken under Part 2 of PACE could only be used for the ‘law enforcement purposes’ set out above.

#### **Exclusions for certain regimes (section 17)**

40. Amended PACE by inserting section 63U which disapplies the PACE regime (as amended by the Protection of Freedoms Act) in relation to DNA and fingerprints taken under certain other regimes, such as the Terrorism Act 2000 or the International Criminal Courts Act 2001, which are themselves amended by the Protection of Freedoms Act to make equivalent self-standing provision within those regimes.

41. Section 63U was amended by section 146 of ASBCPA (see above section on the power to retain samples which are, or may become, disclosable under the Criminal Procedure and Investigations Act 1996 (“CPIA”) under Drafting Issues).

#### **Interpretation and minor amendments of PACE (section 18)**

42. Amended sections 65(1), (2) & 65A of PACE and inserted section 65A to define various terms used in this part of the Protection of Freedoms Act. We are not aware of any current issues with the operation of this section.

#### **Amendments of regimes other than PACE (section 19 and Schedule 1)**

43. This section gives effect to Schedule 1, which makes amendments to various regimes other than the regime inserted into PACE by the Protection of Freedoms Act, under which biometric material may be taken and retained. It follows the same principles as the regime inserted into PACE by sections 1 to 18, whereby material must be deleted if it is not held on a clear statutory basis provided by the Protection of Freedoms Act, and like that regime it has had the effect intended by Parliament. Schedule 1 replicates the national security determination system (see above) in relation to biometric material taken or held under the Terrorism Act 2000 and the Counter-Terrorism Act 2008.

#### **The Commissioner for the Retention and Use of Biometric Material (sections 20 & 21)**

44. These sections established the post of Biometrics Commissioner. Both the initial and current Commissioner have provided robust scrutiny of the regime set out under the Protection of Freedoms Act.

#### **Guidance on making national security determinations (section 22)**

45. This section requires the Secretary of State to issue guidance about the making or renewing of national security determinations, under any provision in the

Protection of Freedoms Act which provides a power to do so. Guidance has been issued under this section.

### **Inclusion on Database (section 23)**

46. Amended PACE by inserting section 63AA which requires the inclusion of profiles on the National DNA Database. We are not aware of any current issues with the operation of this section of the Protection of Freedoms Act.

### **National DNA Database Strategy Board (section 24)**

47. Amended PACE by inserting section 63AB which required establishment of the National DNA Database Strategy Board. The Strategy Board had existed for some years prior to the Protection of Freedoms Act but this put it on a statutory basis. The Board has provided an extremely effective oversight of the new regime. It has issued guidance on retention under the new regime and applications to the Biometrics Commissioner. It has also published Governance Rules which are currently being revised. The Strategy Board has now taken on responsibility for fingerprints and has been renamed the National DNA Database and Fingerprint Strategy Board.

### **Material taken before commencement (section 25)**

48. This section provided a power for the Secretary of State to make transitional, transitory or saving provisions by Order. This section requires the Secretary of State to make such provision securing certain matters in relation to material taken before the commencement of the Protection of Freedoms Act. Five different statutory instruments were passed governing the destruction of material taken prior to the Protection of Freedoms Act coming into force, three of which relate to non-terrorism and two to terrorism related material. The transitional period initially provided in relation to national security material in Great Britain was extended by a year, from 31<sup>st</sup> October 2015 to 31<sup>st</sup> October 2016, to allow for completion of the review of legacy material (see above). We are not aware of any other difficulties with the operation of this section of the Protection of Freedoms Act.

## **PART 1 – REGULATION OF BIOMETRIC DATA**

### **Chapter 2** Protection of biometric information of children in schools etc

#### **Introduction:**

1. 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.
2. The Programme for Government (section 3: civil liberties) stated that the Government "will outlaw the finger-printing of children at school without parental permission".
3. A number of schools in England and Wales 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 was no requirement, in the case of a person aged under 18 years, for consent also to be obtained from the data subject's parents.

#### **Implementation:**

4. Part 1, Chapter 2 (sections 26 – 28) of the Protection of Freedoms Act 2012 introduced duties on any school, sixth-form, 16-19 academy, or further education college that uses automated biometric recognition systems in relation to children under 18. These duties were brought into force on 1 September 2013.
5. The Department for Education published guidance, *Protection of children's biometric information in schools*<sup>11</sup>, in December 2012, to make clear that schools would no longer be able to use pupils' biometric data without parental consent.

---

<sup>11</sup> <https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>.

6. At that time the then Department for Business, Innovation and Skills had intended to provide separate guidance to further education colleges with under-18 students. It intended to largely reproduce the guidance provided to schools to explain the requirements on further education colleges. This guidance was not published and the Department for Education is therefore planning to amend its existing guidance shortly to reflect the legal obligations on further education colleges with under-18 students on roll.
7. In the interim, the existing guidance continues to be available.

### **Preliminary assessment of the Act:**

8. Prior to the introduction of the Protection of Freedoms Act, the Department for Education was aware of concerns about the sensitivity surrounding the use of biometric technologies. The Big Brother Watch report, *Biometrics in schools*<sup>12</sup>, provided details of the likely proportion of schools consulting parents before enrolling children into a biometric system. This research confirmed previous estimates provided in the media by interest groups<sup>13</sup>, which had suggested that around 30% of secondary schools and 5% of primary schools were using these systems.
9. The Department for Education's guidance was not published with the intention of limiting the use of biometric technologies, which can have significant benefits to schools and colleges, including contributing to site safety and the speed and ease of access to services such as school meals. Its objective, as are the relevant sections of the Act, was to leave schools and colleges in no doubt of their responsibilities when it comes to young people's data, making clear that parental consent was required before information can be collected.
10. Since the publication of its guidance, the Department for Education has not received any significant representations about the use of biometric technologies

---

<sup>12</sup> <https://bigbrotherwatch.org.uk/2014/01/one-million-pupils-fingerprinted-school/>.

<sup>13</sup> Clark, L. (2010) One in three secondary schools fingerprinting pupils as Big Brother regime sweeps education system' *Mail Online*. Available at: <http://www.dailymail.co.uk/news/article-1285305/One-schools-fingerprinting-pupils-Big-Brother-regime-sweeps-education-system.html>. Information published on [www.leavethemkidsalone.com](http://www.leavethemkidsalone.com) by the pressure group *Leave them kids alone* no longer available.



in schools or colleges. Accordingly, it is satisfied that the legislation has had the desired effect, i.e. it has informed schools and colleges of their obligations and there is no evidence that the legislation has had a negative impact on schools and colleges, or on young people.

11. The House of Commons' Science and Technology Committee, in its March 2015 report, Current and future uses of biometric data and technologies<sup>14</sup>, cited some use of biometrics in schools when drawing the Government's attention to issues of proportionality (paragraphs 57-61). The Government's response on this matter, under the heading 'Public Attitudes' (Recommendation 5) was provided by the Home Office in Current and future uses of biometric data and technologies: Government Response to the Committees Sixth Report of Session 2014-15, published in September 2015.

---

<sup>14</sup> HC 734, published on 7 March 2015:  
<https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf>.

<sup>15</sup> HC 455, published on 16 September 2015: <http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/biometrics-sr-to-be-published/>.

## **PART 2 – REGULATION OF SURVEILLANCE**

### **Chapter 1: Regulation of CCTV and other surveillance camera technology**

Introduction:

1. The 2010-15 coalition Liberal Democrat and Conservative Programme for Government (section 3: civil liberties) states that the Government “*will further regulate CCTV*”.
2. CCTV systems (including Automatic Number plate Recognition (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 Data Protection Act 1998 (DPA). The Information Commissioner’s Office (ICO) has also issued guidance to CCTV operators on compliance with their legal obligations under the DPA. 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). On 15 December 2009, the then Labour Government announced the appointment of an interim CCTV Regulator (Hansard, House of Commons, columns 113WS-114WS).
3. The joint role of interim CCTV regulator and Forensic Science Regulator (FSR) was previously held by Andrew Rennison, who was subsequently appointed as Surveillance Camera Commissioner (SCC) under section 34 of the Protection Of Freedoms Act 2012 in September 2012. The purpose of the role is to promote compliance with the Surveillance Camera Code of Practice, issued under section 30 of the Protection of Freedoms Act, and provide advice on it. Domestic use of CCTV and covert surveillance is not covered in the remit of the SCC. Domestic use is covered by the ICO and covert use by the Office of Surveillance Commissioners. Mr Rennison played a key role in the development of the surveillance camera code of practice, which was published in June 2013 to provide guidance on the appropriate and effective use of surveillance camera systems. In 2013, Ministers agreed that the role of SCC and FSR should be split into two separate roles. Mr Rennison had fulfilled his statutory functions alongside a non-statutory role as Forensic Science Regulator (FSR). This was a full time arrangement, and had been successful whilst the code of practice had

been under development. However, since the code had come into force, the demands made upon the surveillance camera commissioner were expected to change and increase. Mr Rennison's term of office ran until February 2014. On 10 March 2014 Tony Porter, QPM was appointed as SCC.

## **Implementation**

4. Mr Porter's initial appointment as SCC on 10 March 2014 was made by the then Home Secretary under the Protection of Freedoms Act for a three year tenure. This was extended on 10 March 2017 for a further three years. The role of the SCC is to encourage voluntary adoption and compliance with the Surveillance Camera Code of Practice, review the effectiveness of the code and provide advice to Ministers if the code requires amending. The Commissioner has had some success in encouraging Relevant Authorities (as specified under the Protection of Freedoms Act) to show due regard to the code alongside promoting voluntary compliance. He has done this by proactive communication of the code which has included creation and promotion of a self assessment tool for public space users of CCTV to self assess themselves against the code.
5. In accordance with his statutory duties and requirements under the Protection of Freedoms Act, the SCC completed a review into the impact and operation of the Surveillance Camera Code of Practice, in February 2016, making a series of recommendations following his review. The SCC proposed a number of amendments to be made to the code, including introducing additional powers which may have required changes to the Protection of Freedoms Act 2012. Ministers did not support adding other public bodies to the list of Relevant Authorities, preferring to keep the code as one that the majority of users of public space surveillance camera systems are encouraged to voluntarily adopt and comply with.
6. Ministers advised that they would prefer to maintain the original commitment made that any legislation should be light touch. The SCC has also created and published self assessment tools for public space users of CCTV, Automatic Number Plate Recognition (ANPR) and Body Worn Video Cameras (BWV) to self assess themselves against the code.

7. The SCC published a Surveillance Camera Strategy for England and Wales on 14 March 2017 which includes delivery plans focussed on improving compliance for Police, Local Authorities and Voluntary Adopters.
8. Following the introduction of the Protection of Freedoms Act, the ICO updated their guidance *"In the picture: a data protection code of practice for surveillance cameras and personal information"* in May 2015.

### **Preliminary assessment of the Act:**

9. The SCC does not have powers of enforcement, as his role is to encourage users of public space CCTV to voluntarily adopt and comply with the code. The SCC has suggested on a number of occasions (including in his review) that some of the code should be mandatory and that all public bodies should be added to the list of Relevant Authorities. Relevant Authorities (as defined in the Protection of Freedoms Act) must show due regard to the code. The decision not to grant statutory powers of enforcement to the SCC under the Protection Of Freedoms Act was challenged during the passage of the legislation and also in responses to consultation on the Surveillance Camera Code of Practice. The rationale for not providing enforcement powers was that breaches of the code could be referred to the ICO, who does have such powers, (where data protection breaches are evident) for investigation as a breach of the DPA. It also ensures that users of public space surveillance camera systems are not burdened with dual regulation.
10. There has been some confusion regarding the role of the SCC and the ICO. This was highlighted in the ICO's response to the consultation on the SCC's review of the Surveillance Camera Code of Practice dated 29 July 2015.
11. There is an overlap in the roles, given that the ICO already oversees the privacy aspect of surveillance camera systems and can take enforcement action under the DPA for any breaches. The ICO and the SCC recently agreed in a revised Memorandum of Understanding to work closer together to clarify any confusion over their roles, and how they can work better together to fulfil their statutory duties and provide a better public service.
12. There have been some notable achievements from the SCC since he began his tenure. The SCC has succeeded in raising awareness of and compliance with the Surveillance Camera Code of Practice by creating a self assessment tool for

public space users of CCTV to self assess themselves against the code, identify areas of non compliance and take steps to resolve the areas identified to demonstrate full compliance. This has been well received by local authorities with a willingness to complete the self assessment to demonstrate compliance. The SCC has also published self assessment tools for ANPR and BWV and a surveillance camera strategy for England and Wales, within the remit of the Protection of Freedoms Act.

## **PART 2 – REGULATION OF SURVEILLANCE**

### **Chapter 2: Safeguards for RIPA surveillance**

#### **Introduction:**

1. Chapter 2 of Part 2 of the Protection of Freedoms Act amended the Regulation of Investigatory powers act (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 RIPA, namely the acquisition and disclosure of communications data, and the use of directed surveillance and covert human intelligence sources (“CHIS”). In Scotland approval is granted by a sheriff’s court.

#### **Implementation:**

2. In October 2012, ahead of the provisions coming into force, the Home Office issued three guidance documents on the new processes: guidance to local authorities in England and Wales; guidance to magistrates’ courts in England and Wales; and guidance to local authorities in Scotland. The amendments were brought into force on 1 November 2012.

#### **Preliminary assessment of the Act:**

3. Local authorities are now applying the changes introduced by the Protection of Freedoms Act and obtaining magistrates’ approval for authorisation of directed surveillance and CHIS and of the acquisition of communications data.
4. The Office of Surveillance Commissioners reviews public authority use of the RIPA powers of directed surveillance and CHIS. The 2014 – 2015 Annual Report considered the impact of the changes in the Protection of Freedoms Act and questioned whether the additional scrutiny of magistrate authorisation was necessary. The Commissioner concluded that: “I remain to be convinced of the value of this additional approval procedure which, obviously, promotes delay.”
5. The Interception of Communications Commissioner, who oversees the acquisition of communications data by public authorities under RIPA, in his 2012 Annual Report noted that: “I have previously reported that I was unconvinced that the Government’s proposals to require all local authorities to obtain judicial

approval before they can acquire communications data would lead to increased standards or have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data...Regrettably the evidence that has been shared with my office to date reinforces my standpoint.”

6. In its submission of March 2015 to a review of Investigatory Powers being carried out by David Anderson QC, the Magistrates’ Association considered that judicial approval “ensures greater consistency of decision-making” and “provides greater confidence in the legitimacy and fairness of the process”.
7. In his final report “A Question of Trust” published in June 2015 – David Anderson QC stated that: “Having spoken to a number of local authority trading standards experts, my impression is that communications data is not uniformly used as much as it could usefully be, and that the cost and delay inherent in obtaining the permission of a magistrate functions as a deterrent to applications that could properly and fruitfully be made”.
8. His report recommended that “The requirement in RIPA 2000 SS23A-B [for magistrate approval of local authority communications data requests] should be abandoned. Approvals should be granted, after consultation with NAFN [National Anti-Fraud Network], by a DP [designated person] of appropriate seniority within the requesting public authority”.
9. The Home Office occasionally receives requests for advice or guidance from both local authorities and magistrates courts on the operation of the arrangements and this is provided on request. The Home Office has noted the comments made by the RIPA oversight Commissioners and David Anderson QC above, but we consider that it remains necessary to ensure that the powers are used in an appropriate way and to provide public reassurance that their use by local authorities would be limited to matters of more serious concern.
10. The Government has recently launched a public consultation on the changes it intends to make to the Investigatory Powers Act 2016 in response to the European Court of Justice’s judgment relating to the Judicial Review of the Data Retention and Investigatory Powers Act 2014. As part of these proposals the government will be creating an independent body, sitting under the Investigatory Powers Commissioner, to authorise communications data requests. This body will authorise the majority of communications data requests, including all

requests made by local authorities. This will replace the requirement for magistrate approval for local authority communications data requests.

11. The surveillance provisions in Part 2 of RIPA, and the changes made to those provisions by the Protection of Freedoms Act, remain in force.



## **PART 3 - PROTECTION OF PROPERTY FROM DISPROPORTIONATE ENFORCEMENT ACTION**

### **Chapter 1 - repealing and amending powers of entry**

#### **Introduction:**

1. Chapter 1 of Part 3 made provision in respect of powers to enter land or other premises and associated powers. 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 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.
2. A “power of entry” means a statutory power (however expressed) to enter land or other premises. It includes any safeguard which forms part of the power. It is usually conferred on a state official of a specified description, for example, police officers, local authority trading standards officers, or the enforcement staff of a regulatory body. It usually empowers the official to enter into a private dwelling, business premises, land or vehicles (or a combination of these) for defined purposes, for example, to search for evidence as part of an investigation, or to inspect the premises to ascertain whether regulatory requirements have been complied with.
3. An “associated power” means a statutory power which is connected with a power of entry and is a power to do anything on, or in relation to, the land or premises or a person or thing found on the land or premises, or otherwise do anything in connection with the power of entry. It includes any safeguard which forms part of the associated power. For example, a power to seize property found on a premises after using a power of entry is an associated power.
4. The objective of the provisions was to allow the repeal of unnecessary powers of entry, the addition of safeguards and the rewriting of powers of entry with a view to consolidating a number of powers in a similar area coupled with the inclusion of extra safeguards. The purpose of doing so was to ensure that state powers of

entry into people's homes or business premises are reasonable and proportionate.

5. In the case of Northern Ireland, the Secretary of State for Northern Ireland has responsibility for reserved powers of entry contained within the Justice and Security (NI) Act 2007. The purpose of the 2007 Act was to deliver a number of measures which were deemed necessary to the commitment to the security normalisation in NI, whilst at the same time ensuring that the necessary powers were in place to protect the public.

### **Implementation:**

6. Other than in relation to Wales and Welsh Ministers, sections 39 to 52 came into force on 1st July 2012, by virtue of section 120 of the Protection of Freedoms Act and S.I. 2012/1205. The operation and commencement of the provisions in relation to Wales are the responsibility of the Welsh Ministers.
7. The power in section 39 (repealing powers of entry) has not been used to date. The powers in section 40 (adding safeguards to powers of entry) and 41 (re-writing powers of entry) have been used once – see S.I. 2015/982. Sections 43 to 46 are supplementary provisions in relation to these powers. Where more appropriate to do so, changes to powers of entry have been made using existing powers or primary legislation.
8. Under section 42, Cabinet Ministers were to undertake a review of existing powers of entry and associated powers. The Home Office co-ordinated the government-wide review including presenting two progress reports to Parliament comprising information submitted by departments. The first progress report was published in January 2013<sup>16</sup>. The second progress report was published in July 2013<sup>17</sup>. Ministers of each department laid their final reports in Parliament on 27 November 2014<sup>18</sup> which show that a total of 1,237 powers of entry were subject to review. Government proposed a significant reduction in the overall number of powers which will leave a total of 912. Government also proposed that, where necessary, remaining powers would have additional safeguards added to ensure

---

<sup>16</sup> <https://www.gov.uk/government/publications/first-progress-report-review-of-powers-of-entry>

<sup>17</sup> <https://www.gov.uk/government/publications/second-progress-report-review-of-powers-of-entry>

<sup>18</sup> <https://www.gov.uk/government/collections/reviews-of-all-powers-of-entry>

appropriate use of the powers. The number of powers for which it was proposed to add further safeguards is 231.

9. Under section 47 the Secretary of State must prepare a code of practice containing guidance about the exercise of powers of entry and associated powers. Section 48 required the code to be laid before Parliament, together with a draft of the order bringing the code into force. The code was laid before Parliament on 8th December 2014. Following the approval of Parliament, the code came into force on 6th April 2015.<sup>19</sup> The code applies to any person exercising a power of entry or associated power, other than a devolved power of entry or devolved associated power, unless such exercise is subject to a separate code of practice issued (however described) under any enactment (whenever passed or made). The code provides guidance and sets out considerations that apply to the exercise of powers of entry including, where appropriate, the need to minimise disruption to business. It is intended to ensure greater consistency in the exercise of powers of entry, and greater clarity for those affected by them, while upholding effective enforcement. Sections 49 to 52 are supplementary provisions in relation to the code.
10. The Protection of Freedoms Act 2012 (Commencement No. 1) Order 2012 (S.I. 2012/1205) commenced sections 39 to 52 on 1st July 2012, other than in relation to Wales and Welsh Ministers, insofar as not commenced by virtue of section 120.
11. The Protection of Freedoms Act 2012 (Code of Practice for Powers of Entry and Description of Relevant Persons) Order 2015 (S.I. 2015/240) brought into force a code of practice for powers of entry, which the Secretary of State is required to prepare, pursuant to section 47(1) and defined “relevant persons” who must have regard to that code.
12. The Council Tax and Non-Domestic Rating (Powers of Entry: Safeguards) (England) Order 2015 (S.I. 2015/982) was made under sections 40 and 41.

### **Preliminary assessment of the Act:**

---

<sup>19</sup> The code of practice is available at <https://www.gov.uk/government/publications/powers-of-entry-code-of-practice>. The Order bringing the code of practice into force is available at [http://www.legislation.gov.uk/ukSI/2015/240/pdfs/ukSI\\_20150240\\_en.pdf](http://www.legislation.gov.uk/ukSI/2015/240/pdfs/ukSI_20150240_en.pdf). Further information about the code of practice is available in the Explanatory Memorandum to the Order, available at [http://www.legislation.gov.uk/ukSI/2015/240/pdfs/ukSIEM\\_20150240\\_en.pdf](http://www.legislation.gov.uk/ukSI/2015/240/pdfs/ukSIEM_20150240_en.pdf).

13. The powers in sections 39 to 41, which provide tools to amend existing powers of entry, have been used on one occasion to date. Departments responsible for the legislation providing for powers of entry are best placed to determine how to implement changes. For example, the consolidation of over 100 separate Trading Standards powers of entry and inspection into a single set of powers was delivered alongside a package of measures via primary legislation in the Consumer Rights Act 2015.
14. Cabinet Ministers completed and laid reports before Parliament on 27 November 2014 in relation to a total of 1,237 powers of entry subject to review. In these detailed reports Ministers proposed a significant reform of the existing powers of entry landscape which Departments are continuing to implement.
15. The Home Office operates a gateway process for departments seeking to introduce new powers. This ensures that any new powers are necessary and include proportionate safeguards consistent with the approach taken during the review. All new, amended or re-enacted powers of entry must now be submitted to the Home Office for ministerial approval. If approved, the power still needs to undergo parliamentary scrutiny. Guidance has been issued in relation to new or amended powers of entry<sup>20</sup>, which is primarily aimed at people working in central government departments and agencies, who are thinking about creating, amending or re-enacting powers of entry. Government departments and agencies need to complete a form<sup>21</sup> setting out the background, necessity, proportionality and safeguards attached to the powers and submit it to the powers of entry gateway team. The Home Office then considers the application and may ask for further clarification before recommending ministers approve or not approve the new power.
16. We are not aware of any failure to adhere to the code of practice under section 47, or any civil or criminal proceedings which take account of a failure to have regard to the code.

---

<sup>20</sup> Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/98386/powers-entry-guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/98386/powers-entry-guidance.pdf).

<sup>21</sup> Available at <https://www.gov.uk/guidance/powers-of-entry>.

17. A review of the code of practice is expected to take place five years following introduction. There have been no revisions to the code. There have been no calls for the code of practice to be modified.
18. In the case of Northern Ireland, after reviewing the powers of entry in the 2007 Act in 2014, the Secretary of State for NI concluded that they remain necessary and proportionate to protect the public in the face of an ongoing security threat in NI. The Secretary of State was confident that robust safeguards ensure the powers are used correctly and only where necessary and proportionate; as well as a Code of Practice for the powers (published 2013) all powers in the 2007 Act are subject to annual independent review.
19. The review of these powers of entry was published in a report and laid in Parliament by the Secretary of State in November 2014. The report summarised the powers, considered their necessity and proportionality, the extent of their use, safeguards (including a Code of Practice), post legislative scrutiny, authorisation procedures and records. The report made clear that as a result of the review, there was no intention to repeal, re-write or introduce further safeguards to the powers at that time. It was also made clear that the Independent Reviewer of the 2007 Act is able to make recommendations to the Secretary of State on the powers and any such recommendations will be considered and the necessary action taken. That action could take the form of a repeal, re-write or the inclusion of further safeguards, if it became necessary and appropriate.

## **PART 3 - PROTECTION OF PROPERTY FROM DISPROPORTIONATE ENFORCEMENT ACTION**

### **Chapter 2: offence concerning vehicles left on land; power to remove vehicles; recovery of unpaid parking charges**

#### **Introduction:**

1. The Programme for Government (section 30: transport) stated that the Government “*will tackle rogue private sector wheel clampers*”. Chapter 2 made provision in respect of parking enforcement. It made it a criminal offence to immobilise a vehicle, move a vehicle or restrict the movement of a vehicle without lawful authority.
2. It made provision to extend the power to make regulations for the police and others to remove vehicles that are illegally, dangerously or obstructively parked.
3. It provided 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.

#### **Implementation:**

4. Chapter 2 of Part 3 of the Protection of Freedoms Act 2012 deals with vehicles left on land. Section 54, makes it an offence to clamp, remove or otherwise immobilise a vehicle without lawful authority in England and Wales. Section 55, gives the Secretary of State a power to make regulations allowing named authorities (such as the police), to remove vehicles from private land; and 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.
5. Following the banning of vehicle clamping under this Act, it was necessary to put in place an alternative system whereby private landowners could recover parking charges. This was achieved by Schedule 4 which 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.

6. The first condition 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. The second condition is that the creditor must have served the appropriate notices as set out in paragraphs 7 and 8 or 9 of the Schedule. The third condition (which applies only to registered vehicles) 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. The fourth condition is that if any requirements are prescribed for the display of parking notices on private land they must have been complied with prior to the period of parking in question. The provisions came into force on 1 October 2012.
7. In September 2012, the Department for Transport published the following non-statutory guidance on S56 and Schedule 4 of the Act available online at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/9155/guidance-unpaid-parking-charges.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/9155/guidance-unpaid-parking-charges.pdf)
8. MHCLG reviewed operation of the scheme in 2015 by virtue of a “call for evidence” consultation. They are proposing new measures to improve the way private parking operates in England

### **Preliminary assessment of the Act**

9. The Protection of Freedoms Act provisions on private wheel clamping removed opportunities for direct enforcement from landowners, meaning landowners turned to indirect forms of parking management and enforcement.
10. The general increase in numbers of DVLA disclosures of vehicle keeper data recorded in the table below have a number of contributing factors:
  - Firstly, the Protection of Freedoms Act 2012 made wheel clamping and vehicle removal on private land unlawful (in the absence of lawful authority) and introduced keeper liability for parking charges, likely to be the main driver of increased volumes of DVLA disclosures of vehicle keeper data to private parking operators.

- Secondly, increased use of automatic number plate recognition (ANPR) cameras, replacing windscreen tickets containing the parking charge notice, meaning alleged contraventions require DVLA vehicle keeper data to contact the registered keeper via post.
- Thirdly, increasing commerce and the increased use of cars on the road may have contributed to the need for more parking management.
- It is also thought that there has been an increase in landowners entering into agreements with parking companies where the landowner pays little or nothing for parking management services, while the parking company keeps the income from enforcement. There is currently no government regulation of such arrangements, thus they are quite lawful.

11. The figures below are also management information and so cannot be broken down into disclosures relating to civil claims using the Protection of Freedoms Act keeper liability powers. They also include disclosures for the pursuit of charges by private parking operators that are not using the additional powers in PoFA.

<b>Financial Year</b>	<b>Requests (millions)</b>
2012/13	1.8
2013/14	2.4
2014/15	3.1
2015/16	3.7
2016/17	4.7

DVLA disclosures of vehicle keeper data (source: DVLA, DFT)

12. Responsibility for this area of legislation transferred to MHCLG in 2015. The government is supporting new legislation to regulate the private parking industry. Parking (Code of Practice) is a Private Members Bill presented by Sir Greg Knight MP which seeks to introduce regulation to the sector. It had its Presentation and First Reading (Standing Order No. 57) on 19th July 2017 and its Second Reading on 2 February 2018. Under the plans, which will deliver on a manifesto commitment to tackle rogue parking operators, a stringent new Code of Practice will be developed by the Secretary of State in conjunction with motorists groups and other experts. Those falling foul of the rules would then be blocked from accessing driver data and issuing fines, effectively forcing them out of the industry.

13. These measures build on action government has already taken to tackle rogue private parking operators, including banning wheel clamping and towing, and over-zealous parking enforcement by councils and parking wardens.



## **PART 4 – COUNTER-TERRORISM POWERS**

### **Introduction:**

1. 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<sup>22</sup>, setting out a number of counter-terrorism and security powers to be considered by the review.
2. The Home Secretary reported the outcome of the review<sup>23</sup> 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<sup>24</sup>. Chapter 2 of Part 2, and Part 4 of the Protection of Freedoms Act, gave effect to the review's conclusions in respect of the use of powers under the Regulation of Investigatory Powers Act 2000 by local authorities, police stop and search powers under the Terrorism Act 2000, and the maximum period of pre-charge detention for terrorist suspects under the Terrorism Act 2000.
3. Section 57 amended the Terrorism Act 2000 so that the maximum period of pre-charge detention for terrorist suspects arrested under that Act was reduced from 28 to 14 days, reflecting the conclusion of the review that the longer period was not routinely necessary.
4. The Review also concluded that it may be necessary temporarily to revert the pre-charge detention period to 28 days in exceptional circumstances, for example in response to multiple co-ordinated attacks or during multiple large and simultaneous investigations, and that draft emergency legislation should be

---

<sup>22</sup><http://www.homeoffice.gov.uk/publications/counter-terrorism/ct-terms-of-ref/counter-terrorism-terms-of-ref?view=Html>

<sup>23</sup><http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/review-findings-and-rec?view=Binary>

<sup>24</sup> <http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/report-by-lord-mcdonald?view=Binary>

prepared so that it could be introduced in these circumstances. Two Draft Detention of Terrorism Suspect (Temporary Extension) Bills were published<sup>25</sup>, to reflect the legislative position before and after passage of the Protection of Freedoms Act, and were subject to pre-legislative scrutiny by a Joint Committee, the report of which was published on 23 June 2011<sup>26</sup>. Section 58 provides an Order-making power for the Secretary of State to bring into force the regime envisaged by the draft emergency legislation, for a maximum period of three months, at a time when Parliament is not able to consider the draft Bill because it is dissolved or in the period before the first Queen's Speech of a new Parliament.

5. Section 59 repealed sections 44 to 46 of the Terrorism Act 2000, which provided a power for senior police officer to authorise the stop and search of people and vehicles within a specified area, without suspicion, for articles of a kind which could be used in connection with terrorism. An authorisation could be made where the senior officer considered it expedient for the prevention of acts of terrorism. The Review found that this had proved a useful power but identified a number of concerns around its breadth, the scale and impact of its use, and its overall necessity. The Review therefore recommended it be repealed and replaced with a more tightly circumscribed stop and search power.
6. The repealed power had also been successfully challenged at the European Court of Human Rights (ECtHR). In the case of *Gillan and Quinton v UK* (*Application no. 4158/05*), brought by two individuals stopped and searched under section 44 of the 2000 Act in 2003, the ECtHR found that the powers violated Article 8 of the European Convention on Human Rights 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.
7. Section 60 inserted section 43A to the Terrorism Act 2000, building on the existing power at section 43 of the 2000 Act to stop and search a person on suspicion that they are a terrorist, by providing an equivalent power to search vehicles. This filled a gap which had become apparent through the operation of the powers, and responded to a further recommendation of the Review.

---

<sup>25</sup> <https://www.gov.uk/government/publications/draft-detention-of-terrorist-suspects-temporary-extension-bills>

<sup>26</sup> <https://www.publications.parliament.uk/pa/jt201012/jtselect/jtdetent/161/161.pdf>

8. Section 61 inserted section 47A to the Terrorism Act 2000, providing a new stop and search power to replace that repealed by section 59. Under the section 47A power a senior officer may authorise the stop and search of persons and vehicles without suspicion, for the more limited purpose of discovering if they have anything in their possession, or if a vehicle contains anything, which may constitute evidence that they are a terrorist or that the vehicle is being used for the purposes of terrorism. The replacement power also places greater constraints on the making of such authorisations. The officer making the authorisation must have a reasonable suspicion that an act of terrorism will take place within the area covered by it, and the size of the area and the duration of the authorisation must be no greater than is necessary to prevent the Act of terrorism.
9. Section 62 inserted section 47AA to the Terrorism Act 2000, requiring the Secretary of State to issue a Code of Practice for the operation of the stop and search powers in the 2000 Act.

### **Implementation**

10. All of Part 4 was commenced by the Protection of Freedoms Act 2012 (Commencement No.1) Order 2012 (2012 No.1205). Section 62 was brought into force on 9 May 2012, and Sections 57 to 61, and 63, were brought into force on 10 July 2012.
11. The Independent Reviewer of Terrorism Legislation is responsible for reviewing the operation of the Terrorism Act 2000, including the provisions inserted by the Protection of Freedoms Act. He is required to report annually to the Home Secretary on this, and the Home Secretary is required to lay his reports before Parliament. The most recent such report was published on 1 December 2016<sup>27</sup> and made one recommendation in relation to Part 4 of the Protection of Freedoms Act: that statistics should be published for the use of the stop and search power provided by section 60 of the Protection of Freedoms Act by a wider range of police forces. The Government responded formally to the report on 20 July 2017, accepting this recommendation.
12. A code of practice for the operation of the stop and search powers in the Terrorism Act 2000 in England, Wales and Scotland, was issued on 10 July

---

<sup>27</sup> <https://www.gov.uk/government/publications/the-terrorism-acts-in-2015>

2012<sup>28</sup>, under section 47AB of the 2000 Act, as inserted by section 61 of the Act. This was brought into force by the Terrorism Act 2000 (Codes of Practice for the Exercise of Stop and Search Powers) Order 2012 (2012, No.1794).

13. The powers are different in Northern Ireland, the Protection of Freedoms Act amended the powers to stop and search 'without reasonable suspicion' contained in both the Justice and Security (NI) 2007 Act and the Terrorism Act 2000.
14. Paragraph 4A of Schedule 3 to the 2007 Act allows the police to stop and search a person in an authorised area or place without reasonable suspicion, for the purpose of ascertaining whether they are in unlawful possession of munitions or in possession of wireless apparatus. The 2007 Act also allows a member of Her Majesty's forces who is on duty to stop and search a person for the same purpose in a public place, and this power is not subject to an authorisation regime. The 2007 Act powers are specific to Northern Ireland.
15. As a result of the Protection of Freedoms Act, before police officers can stop and search individuals without reasonable suspicion under the 2000 Act or the 2007 Act a senior police officer must first authorise the use of the powers, for a limited period and in a designated area or place. That authorisation must be confirmed by the Secretary of State (or someone with their delegated authority) if it is to last for longer than 48 hours. Authorisations cannot last for more than 14 days.
16. Since the authorisation procedure was introduced in July 2012, authorisations under the 2007 Act have been in place in Northern Ireland except for a period in May 2013 when the PSNI made use of the without suspicion 2000 Act powers. Each authorisation has been confirmed by the Secretary of State's authority and has extended to the whole of NI, considered necessary and proportionate in light of the severe threat reported in successive authorisations.
17. The 2007 Act powers were designed specifically to address the particular nature of the threat in Northern Ireland which is largely munitions-related and extends to crime other than terrorism. This is reflected in part in the different test that applies for making a 2007 Act authorisation.

---

<sup>28</sup> <https://www.gov.uk/government/publications/code-of-practice-for-the-exercise-of-stop-and-search-powers>

18. Under paragraph 4A of Schedule 3 to the 2007 Act, a senior PSNI officer of at least the rank of Assistant Chief Constable (ACC) may give an authorisation for constables to stop and search without suspicion within a specified area or place for up to 14 days. The senior officer may give an authorisation in relation to a specified area or place if he reasonably suspects that the safety of any person might be endangered by the use of munitions or wireless apparatus and reasonably considers that the:

- authorisation is necessary to prevent such danger;
- specified area or place is no greater than is necessary to prevent such danger; and
- duration of the authorisation is no longer than is necessary to prevent such danger.

19. If the authorisation is not confirmed by the Secretary of State within 48 hours then the authorisation lapses meaning the powers may no longer be used. If the Secretary of State confirms the authorisation within that time frame however, the authorisation will remain in effect for the period stated on the form up to a maximum of 14 days (which includes the initial 48 hour window). For all authorisations the Secretary of State must be satisfied that it is necessary and proportionate. The duration and the geographical extent should not be greater than is necessary to prevent the endangerment of the public from munitions or wireless apparatus. The Secretary of State has the power to amend the duration and geographic extent of the authorisation.

### **Preliminary assessment of the Act:**

#### **Pre-Charge Detention of Terrorism Suspects (Sections 57 and 58)**

20. These sections of the Protection of Freedoms Act have worked well. They have ensured that the maximum period of pre-charge detention normally available for suspects arrested under the Terrorism Act 2000 is reduced to the period of 14 days recommended by the Review of Counter-Terrorism and Security Powers (see above). They have also ensured that the Government is able to increase this period to 28 days if necessary in exceptional circumstances of the kind described above. This has ensured a better balance between safeguarding the rights of individuals who have not yet been charged with an offence, and ensuring that strong powers are available to protect the public when justified. It has not been necessary to introduce the emergency legislation or to use the Order making power provided by section 58 of the Protection of Freedoms Act.

## **Stop and Search Powers (Great Britain) (Sections 59 to 62)**

21. These provisions have also worked well. The insertion into the Terrorism Act 2000 of a power to search vehicles on suspicion, equivalent to the existing power to search persons, has helpfully filled an operational gap and has ensured that the police have the powers that they need to protect the public, subject to appropriate safeguards. Use of the power is kept under review by the Independent Reviewer of Terrorism Legislation in his annual reports on the Terrorism Act 2000, and he has not identified any legal or other issues in its operation.
  
22. The repeal of sections 44 to 47 of the Terrorism Act 2000 removed from the statute a power that had proved controversial and that had been found unlawful by the European Court of Human Rights. The Review of Counter-Terrorism and Security Powers concluded that a more limited and focused power to stop and search individuals and vehicles without reasonable suspicion in exceptional circumstances is operationally justified, and in line with its recommendations the Protection of Freedoms Act introduced a replacement power with significant changes to ensure its compatibility with ECHR rights. Reflecting the exceptional nature of the power it has not been used in Great Britain, and has only been used once in Northern Ireland.
  
23. It should be noted that the power is different in Northern Ireland. Since the authorisation procedure was introduced in July 2012, authorisations under the 2007 Act have been in place in Northern Ireland except for a period in May 2013 when the PSNI made use of the without suspicion 2000 Act powers. Each authorisation has been confirmed by the Secretary of State's authority and has extended to the whole of NI, considered necessary and proportionate in light of the threat reported in successive authorisations.
  
24. Legal challenges have been brought against stop and search powers in the 2007 Act and the authorisation procedure introduced. In 2013, the Court of Appeal in the *Canning, Fox and McNulty* JR found that without a Code of Practice in force for the use of stop and question and stop and search powers under 2007 Act, the powers were too broad and lacked adequate safeguards (at that time, the Code was available in draft and was being followed in practice but had not been brought into force in law). Following this judgment, the use of the powers was immediately suspended for a 6 day period, during which an authorisation under section 47A of TACT was given and the TACT stop and search powers were

used. The situation with respect to the 2007 Act powers was rectified by bringing the Code of Practice into force by way of urgent Parliamentary procedure. This Code remains in operation. There is an ongoing challenge to the lawfulness of the 2007 Act powers and the authorisation regime in the case of Ramsey. On 8 May 2014 Mr Justice Treacy dismissed the application. The case then went to the Court of Appeal in April 2015 and fresh grounds of challenge relating to the authorisation regime have been put forward. Following the guidance given by the Court of Appeal in its judgment in Canning, Fox and McNulty on 9 May 2013, PSNI continue to use the powers on the basis that the introduction of the Code of Practice rendered the powers compatible with the ECHR. The case of Ramsey was heard by the Court of Appeal on 20 November 2017 and is awaiting a judicial decision.

25. The without suspicion powers in the 2007 Act remain significant to the PSNI's response to the dissident republican threat in NI, and its wider response to other criminality involving munitions and wireless apparatus (such as activity linked to paramilitarism). The operation of these powers is kept under statutory review by the Independent Reviewer of the 2007 Act. As part of the review, the Reviewer examines stop and search authorisations in detail. As set out in his published reports, the Reviewer continues to be satisfied with the use of the powers under the authorisation procedure, in light of the security situation in NI. Indeed, in his 2016 report the Reviewer stated *"I think that the provisions in the JSA which govern authorisations should be amended to reflect more accurately the ongoing security situation in Northern Ireland which is likely to continue for the foreseeable future. In particular, authorisations should be for at least 3 months provided existing safeguards are retained."* In his most recent report (February 2017) the Reviewer reiterated his recommendation to the Secretary of State to amend the 2007 Act to allow an authorisation to remain in place for at least 3 months provided that the security situation remains as it is and sufficient safeguards remain in place.

## **PART 5 -SAFEGUARDING VULNERABLE GROUPS**

### **Chapter 1, changes to Safeguarding of Vulnerable Groups Act 2006 (“SVGA” & corresponding amendments in NI**

#### **Introduction:**

1. Chapter 1 of Part 5 amended the Safeguarding Vulnerable Groups Act 2006 (“SVGA”) which provides the framework for the vetting and barring scheme operated by the Disclosure and Barring Service (“DBS”) (formerly operated by the Independent Safeguarding Authority (“ISA”)) in England and Wales. The amendments, in particular, repealed 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.

#### **Implementation**

2. The Protection of Freedoms Act 2012 (Commencement No. 2) Order 2012 (SI 2012/2075) brought into force section 78 insofar as it related to paragraphs 3(2) and 14(4) of Schedule 7 on 10 August 2012.
3. The Protection of Freedoms Act 2012 (Commencement No. 3) Order 2012 (SI 2012/2234) brought the following sections of the Protection of Freedoms Act into force on 10 September 2012:
  - Sections 64 to 71;
  - Section 72(4) to (6);
  - Section 75(1) to (2) and (4) to (6);
  - Section 75(3) in so far as it substitutes section 43(3), (4), (5), (5D), (5E), (5F), (5G) and (5H) of the Safeguarding Vulnerable Groups Act 2006;
  - Section 76(1), (2), (3)(f), (4)(f) and (5);
  - Section 77;
  - Section 78 insofar as it relates to paragraphs 1 to 8, 9(4) to (6), 12(1), 12(2) insofar as it substitutes Art. 45(3), (4), (5), (5D), (5E), (5F), (5G) and (5H) into the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007, 12(3) and (4), 13(1), (2), (3)(g), (4)(g) and (5), and 14 of Schedule 7
  - Sections 72(1) to (3), 73, 74, 75(3) (otherwise than in SI 2012/2234), 76(3)(a) to (e) and (4)(a) to (e), and 78 (otherwise than in SI 2012/2075 and SI 2012/2234) are not yet in force.



4. The Protection of Freedoms Act 2012 (Commencement No. 2) Order 2012 (SI 2012/2075) made 7<sup>th</sup> August 2012 commenced provisions in section 78 as it related to paragraphs 3(2) and 14(4) of Schedule 7.
5. The Protection of Freedoms Act 2012 (Commencement No. 3) Order 2012 (SI 2012/2234) made on the 28 August 2012 commenced further provisions in:
  - Sections 64 to 71;
  - Section 72(4) to (6);
  - Section 75(1) to (2) and (4) to (6);
  - Section 75(3) in so far as it substitutes section 43(3), (4), (5), (5D), (5E), (5F), (5G) and (5H) of the Safeguarding Vulnerable Groups Act 2006;
  - Section 76(1), (2), (3)(f), (4)(f) and (5);
  - Section 77;
  - Section 78 insofar as it relates to paragraphs 1 to 8, 9(4) to (6), 12(1), 12(2) insofar as it substitutes Art. 45(3), (4), (5), (5D), (5E), (5F), (5G) and (5H) into the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007, 12(3) and (4), 13(1), (2), (3)(g), (4)(g) and (5), and 14 of Schedule 7.
6. The following statutory guidance, issued by the Secretary of State for Education in accordance with S.77(6), on the supervision of activity with children has been issued: <https://www.gov.uk/government/publications/supervision-of-activity-with-children>. It assists providers of regulated activity when they decide to supervise with the aim that the supervised work will not be regulated activity. It has been in force since 10 September 2012

### **Preliminary assessment of the Act**

7. Chapter 1 of Part 5 made amendments to the SVGA which provides the framework for barring individuals from working with children or vulnerable groups where they may pose a risk of harm. Collectively these amendments remodelled the existing scheme by removing the registration and monitoring requirements, amended the scope of 'regulated activity' and removed the concept of 'controlled activity'.

### **Section 64: Restriction of scope of regulated activities: children**

### **Section 65: Restriction of definition of vulnerable adults**

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

8. The SVGA sets out the extent of 'regulated activity' as it relates to children and adults. Regulated activity is the set of activities that an individual is barred from doing if included in the children's or adult's barred list. An individual may be included in one, or both, of the lists as a result of committing certain serious

offences or as a result of a decision by the DBS that the individual presents a risk of harm.

9. Sections 64 amended the existing definition of regulated activity relating to children in order to reduce the scope of work that barred individuals are prohibited from doing.
10. Section 65 repealed the existing definition of vulnerable adults. It also inserts a new definition such that 'vulnerable adult' means any person aged 18 or over for whom a regulated activity is provided.
11. Section 66 amended the existing definition of regulated activity relating to adults to focus on the nature of the activity, rather than on the setting it may occur in.

#### **Section 67: Alteration of test for barring decisions**

12. This section amended Schedule 3 to the SVGA which sets out how an individual becomes included on children's or adults' barred list. In particular, this section introduced a requirement to seek representations from an individual who has committed an offence specified in regulations governing "automatic bars with representations" before reaching a decision on whether to place them on a list. The section also limited the application of a bar, in relation to these offences or where the individual has been referred to the DBS on the grounds they may pose a risk of harm, to those individuals who are engaged, have been engaged or might in the future be engaged in regulated activity.
13. These changes mean that only those people who have previously worked, or may now be seeking to work, with children or vulnerable adults, and pose a risk of harm to children or vulnerable adults, are included on the barred lists.

#### **Section 68: Abolition of controlled activity**

14. This section abolished the concept of controlled activity. Previously controlled activity had consisted of activities ancillary to work within regulated activity. An employer was required to check if a person was barred from regulated activity before permitting them to work in controlled activity.

#### **Section 69: Abolition of monitoring**

15. This section repealed sections 24-27 of the SVGA which, had they been brought into force, would have required individuals engaged, or seeking to be engaged, in regulated activity to make an application to be monitored. This change abolished the proposed monitoring scheme.

### **Section 70: Information for purposes of making barring decisions**

16. Subsection (1) extended the existing power to obtain relevant conviction and caution information from the police to include circumstances where any relevant paragraphs of Schedule 3 to the Safeguarding and Vulnerable Groups Act 2006 “appears to apply”. This is because it may not be clear at the time of referral whether the criteria for automatic or discretionary barring have been satisfied.

17. Subsection (2) inserted a replacement sub-paragraph (2) into paragraph 20 of Schedule 3 to the SVGA. This required the Secretary of State to send certain information to the ISA when referring a person to the ISA under paragraphs 1, 2, 7 or 8 of that Schedule. Referral under paragraphs 1 or 7 would take place where the Secretary of State had reason to believe that the prescribed criteria for automatic inclusion in a barred list might apply to a person. Referral under paragraphs 2 or 8 would take place where the Secretary of State had reason to believe that the prescribed criteria for inclusion in a barred list subject to representations might apply to a person and that person was or had been, or might in future be, engaged in regulated activity. When certain functions of the ISA and the Secretary of State were transferred to DBS the replacement sub-paragraph (2) was repealed (art.34 SI 2012/3006).

18. These changes update the arrangements for obtaining information for purposes of making barring decisions in order to reflect the needs of the remodelled barring scheme.

### **Section 71: Review of barring decisions**

19. This section provides for the DBS to review an individual’s inclusion in either of the barred lists. Where there has been a change in the individual’s circumstances, new information has come to light or an error identified, the DBS may remove the individual from the list. This has allowed for individuals to be removed from the list in appropriate circumstances, without requiring that

individual to apply for their inclusion to be reviewed. Figures relating to these reviews are not available as the different types of review are not recorded separately.

### **Section 72: Information about barring decisions**

20. This section replaced sections 30 to 32 of the SVGA with new sections 30A and 30B. These new sections have not yet been commenced as the technical capacity is not yet in place to deliver these services.
21. New section 30A will allow persons who fall within Schedule 7 to the SVGA to obtain information indicating whether a person is barred from regulated activity.
22. New section 30B will allow persons who fall within Schedule 7 to the SVGA to register an interest in persons in regulated activity. They will be notified should the individual become barred.

### **Section 73: Duty to check whether person has been barred**

23. This section inserted new section 34ZA into the Safeguarding and Vulnerable Groups Act 2006 which places a duty on regulated activity providers, or personnel suppliers providing persons to work in regulated activity, to ascertain whether a person is barred prior to permitting that person to engage in regulated activity. This duty could be met by obtaining information under new section 30A of the SVGA, obtaining information on an enhanced criminal record certificate in respect of regulated activity or checking such a certificate and checking the status of that certificate via the update service.
24. This section has not yet been commenced as it relies on the un-commenced provisions at section 72.

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

25. This section inserts new paragraphs 5A and 11A into Schedule 3 to the SVGA. These provide that the DBS must not include a person in the barred lists if it knows that the person is included in the corresponding lists maintained under the law of Scotland or Northern Ireland. This is to prevent duplication between lists held in respect of England and Wales, Northern Ireland, and Scotland.

26. Section 74 is not yet commenced as the technical capacity is not yet in place to deliver these services.

### **Section 75: Professional bodies**

27. This section amended the duties on professional bodies, also known as keepers of registers. Subsection 1 replaced the duty on keepers of registers to provide information to the DBS with a discretionary power to do so. Subsection 2 omitted amendments to the Safeguarding and Vulnerable Groups Act 2006 that had not been brought into force. Subsections 4 and 5 made minor amendment to the definition of 'relevant register'.

28. Subsection 6 omitted section 44 of the SVGA which had not been fully commenced. This section provided for arrangements under which the DBS could provide barred list information to keepers of registers. Subsection 3 inserted updated arrangements into section 43 of the SVGA. Of these, new subsections 3 to 5, which provide for an ad hoc application from a keeper of register to check the barred list, are in force. New subsections 1, 2 and 5A to 5C, which provide for proactive notification of an individual's barred list status to a keeper of register, are not yet commenced as the technical capacity is not yet in place to deliver these services.

### **Section 76: Supervisory authorities**

29. This section amended the duties on supervisory authorities as specified at section 45(7) of the SVGA in similar ways to the changes in relation to professional bodies. Again, provisions for the proactive notification of an individual's barred list status are not yet commenced as the technical capacity is not yet in place to deliver these services.

### **Section 77: Minor amendments**

30. This section made further minor amendments to the existing provisions to repeal un-commenced amendments that would have required notification to employers of an intention to place an individual on the barred list; to replace the duty on local authorities to provide information to the DBS with a discretionary power to do so; to enable the DBS to provide information to police forces for various purposes; and to provide for the Secretary of State to issue guidance for providers of regulated activity and personnel suppliers in relation to supervision.

31. Statutory guidance on the supervision of activity with children was issued by the Secretary of State for Education on 10 September 2012.

**Section 78: Corresponding amendments in relation to Northern Ireland**

32. The section applied Schedule 7 which made corresponding amendments in relation to the barring scheme in Northern Ireland. This section is not yet fully commenced because the technical capacity is not yet in place to deliver these services.

## **PART 5 -SAFEGUARDING VULNERABLE GROUPS**

### **Chapter 2, changes to criminal records**

#### **Introduction:**

1. Chapter 2 of Part 5 made amendments to Part 5 of the Police Act 1997 (“the 1997 Act”) which set out the framework for the operation and the disclosure of criminal convictions and other relevant information in certificates issued by the DBS (previously issued by the Criminal Records Bureau (“CRB”)) to support the assessment of a person’s suitability for employment and other roles.
2. The Protection of Freedoms Act 2012 (Commencement No. 1) Order 2012 (SI 2012/1205) brought into force section 85 on 1 July 2012.
3. The Protection of Freedoms Act 2012 (Commencement No. 3) Order 2012 (SI 2012/2234) brought into force on 10 September 2012:
  - Section 79(1);
  - Section 79(2)(b) in so far as it omits section 113B(5) and (6)(b) of the Police Act 1997;
  - Section 79(3) in so far as it inserts section 120AC into the Police Act 1997;
  - Sections 80 to 82;
  - Section 84;
  - Section 86.
4. The Protection of Freedoms Act 2012 (Commencement No. 6) Order 2013 (SI 2013/1180) brought into force section 79(2)(a), the remainder of section 79(2)(b) and (3) and section 83 on 17 June 2013.
5. The Protection of Freedoms Act 2012 (Commencement No. 1) Order 2012 (SI 2012/1205), made 2 May 2012, commences section 85.
6. Police Act 1997 (Criminal Records) (Guernsey) (Amendment) Order 2012 (SI 2012/1762), made 10 July 2012, coming into force in accordance with Art.1(2) to (3)(b). Made under s.118 (and other non-Protection of Freedoms Act powers), extends provisions of Protection of Freedoms Act to Guernsey subject to modifications.

7. The Protection of Freedoms Act 2012 (Commencement No. 3) Order 2012 (SI 2012/2234), made 28 August 2012, commences:
- Section 79(1);
  - Section 79(2)(b) in so far as it omits section 113B(5) and (6)(b) of the Police Act 1997;
  - Section 79(3) in so far as it inserts section 120AC into the Police Act 1997;
  - Sections 80 to 82;
  - Section 84;
  - Section 86.
  - Police Act 1997 (Criminal Records) (Isle of Man) (Amendment) Order 2012 (SI 2012/2598), made 17 October 2012, coming into force in accordance with Art.1(2) and (3). Made under s.118 (and other non-Protection of Freedoms Act powers), extends provisions of Protection of Freedoms Act to Isle of Man subject to modifications.
  - Police Act 1997 (Criminal Records) (Jersey) (Amendment) Order 2012 (SI 2012/2591), made 17 October 2012, coming into force in accordance with Art.1(2) to (3)(b)(Not in force). Made under s.118 (and other non-Protection of Freedoms Act powers), extends provisions of Protection of Freedoms Act to Jersey, subject to modifications.
  - The Protection of Freedoms Act 2012 (Commencement No. 6) Order 2013/1180, made 20 May 2013 brought into force section 79(2)(a), the remainder of section 79(2)(b) and (3) and section 83 on 17 June 2013.

**The following statutory guidance has been issued:**

Title	Date	Detail
Statutory Disclosure Guidance	Effective from 10 September 2012 to 9 August 2015	Issued in accordance with s.82(2)  To assist chief officers of police in making decisions about providing information from local police records for inclusion in enhanced criminal records certificates.



<p>Statutory Disclosure Guidance (second edition)</p> <p>Available at:  <a href="https://www.gov.uk/government/publications/statutory-disclosure-guidance">https://www.gov.uk/government/publications/statutory-disclosure-guidance</a></p>	<p>In force from 10 August 2015</p>	<p>Issued in accordance with s.82(2)</p> <p>Amended to include guidance on disclosing information relating to mental health.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------

8. A legal challenge was brought against section 113B of the Police Act 1997 (which had been amended by section 82(1) of the Protection of Freedoms Act) in the case of *R (on the application of T) v Chief Constable of Greater Manchester* [2014] UKSC 35. However this case did not challenge the particular provisions amended by the Protection of Freedoms Act and is therefore not directly relevant.
  
9. A number of judicial review cases have been brought against individual police forces by applicants challenging the decision by the relevant chief officer under section 113B(4) (as amended by the Protection of Freedoms Act) that certain information is relevant and ought to be included on an enhanced certificate. Similarly, a number of cases have been brought against the Independent Monitor by individuals challenging his decision to uphold the inclusion of information on a certificate. Examples of such cases include *R (on the application of B) v Chief Constable of Hampshire* [2015] EWHC 1238 and *R (on the application of MS) v Independent Monitor of the Home Office* [2016] EWHC 655 (Admin). Such cases challenge individual decisions (for example on the basis of proportionality) rather than challenging the substance of the legislation.

**Preliminary assessment of the Act:**

10. Chapter 2 of Part 5 made amendments to the Part 5 of the Police Act 1997 which provides for the DBS to issue certificates to applicants containing details of their criminal record and other relevant information. These changes, in part, implemented recommendations made by Mrs Sunita Mason in her review of the criminal records regime. Collectively these changes addressed issues concerning the proportionality of the disclosure regime while maintaining employers' ability to make informed recruitment decisions.

## **Section 79: Restriction on information provided to certain persons**

11. Subsection (1) repealed a provision of the Policing and Crime Act 2009 which, if it had been commenced, would have required copies of certain criminal conviction certificates (commonly referred to as a 'basic' check) to be sent to an employer. Subsection (2) repealed provisions of the Police Act 1997 requiring a criminal record certificate or enhanced criminal record certificate to be sent to an employer or registered person.
12. Subsection (3) inserted new sections 120AC and 120AD into the Police Act 1997. New section 120AC provides that DBS may inform a registered person as to the progress of an individual's application for a criminal record certificate or enhanced criminal record certificate (commonly referred to as 'standard' or 'enhanced' checks respectively). The new section 120AD provides that DBS may provide a copy of a certificate to a registered person in certain circumstances
13. The effect of these changes is certificates, at any level, are issued directly to the applicant who may share with a potential employer as they see fit. Previously certificates were also issued to a registered person, an individual registered with the Secretary of State for the purpose of countersigning an application. This has ensured that individuals have ownership of their certificate and can better control who has access to sensitive personal information relating to their criminal history. It also allows for the individual to make necessary representations regarding the information disclosed without the potentially prejudicial impact of an employer already having seen it.

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

14. Subsection (1) introduced a requirement that an applicant for any criminal record check is aged 16 or over. Subsection (2) introduced a requirement that an individual seeking to act as a registered person is aged 18 or over.
15. This age limit was introduced on the basis that children should not be placed in positions susceptible to such checks.

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

16. This section provided further limitations on individuals or organisations seeking to become registered persons allowing for refusal where the individual or

organisation has previously been removed from the register following a breach of the conditions of registration.

### **Section 82: Enhanced criminal record certificates: additional safeguards**

17. This section principally updates the arrangements for disclosure of non-conviction information held locally by police forces.
18. Subsection (1) introduces a higher test for information to be disclosed by a chief officer from 'might be relevant' to 'reasonably believes to be relevant' and ought to be included in the certificate.
19. Subsection (2) provided for the Secretary of State to issue guidance to which chief officers must have regard when making disclosure decisions. The Home Secretary issued Statutory Disclosure Guidance in September 2012 and an updated second edition in August 2015. Implementation of this guidance improved the quality and consistency of disclosure. The guidance is available at <https://www.gov.uk/government/publications/statutory-disclosure-guidance>.
20. These measures have reduced the proportion of certificates issued containing non-conviction information. In the year 2011/12 0.4% of certificates issued included locally held information. In the years following the changes this has reduced to around 0.25% of certificates.
21. Subsection (3) allowed for disclosure decisions to be taken by any chief officer. Where two or more forces hold information about an applicant this would enable the DBS to approach any 'relevant chief officer' to make a decision on disclosure.. Due to technical and operational limitations, decisions continue to be taken by each individual force.
22. Subsections (4) and (5) introduced more robust arrangements for an individual to raise a dispute over the accuracy or relevance of information disclosed on any certificate. This includes a new mechanism to challenge the disclosure of non-conviction information by recourse to the Independent Monitor (IM) – an extension to the functions of the existing role as appointed under section 119B of the Police Act 1997. On making a final decision, the IM has powers to require the issue of a new certificate.

23. The Independent Monitor issues an annual report which includes a summary of cases referred to him. These reports are available at <http://www.gov.uk/dbs>. As a sample, a summary of referrals made between January 2016 and December 2016 is presented below.

<b>Referral figures for January 2016 - December 2016</b>	
Number of cases - waiting for information	8
Number of cases where the IM has made a decision	214
Number of cases withdrawn	21
<b>Total number of cases received</b>	<b>243</b>
<b>Outcomes where the IM made a decision (some cases were outstanding)</b>	
1. Uphold	145
2. Amend	4
3. Deletion	20
4. Partial deletion	18
5. Aged disputes	26
6. Declined to review	1
<b>Total</b>	<b>214</b>

### **Section 83: Updating certificates**

24. This section inserted new section 116A into the Police Act 1997. This section introduced a new service through which employers can check the status of a subscribing applicant's certificate. Checking the status allows an employer to confirm whether an applicant's certificate is up to date or whether new information may be held, in which case the employer should request a new certificate. This service increases the portability of a certificate between roles within the same workforce and reduces costs for individuals undertaking several roles that may be subject to disclosure.

25. The DBS publish extensive information, including details of subscriptions to the update service, at <https://www.gov.uk/government/statistics/dbs-dataset-1-disclosure-progress-information-disclosed-and-update-service-subscriptions>.

The data shows that in February 2017 there were active 972,950 subscribers with employers undertaking around 200,000 status checks each month, significantly reducing the need for individuals to request new certificates when they change role.

### **Section 84: Criminal conviction certificates: conditional cautions**

26. This section provides that details of an unspent conditional caution may be included on a criminal conviction certificate which also discloses details of unspent convictions. 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 85: Inclusion of cautions etc. in national police records**

27. This section amended section 27 of the Police and Criminal Evidence Act 1984 to provide for cautions, reprimands and warnings to be recorded on the Police National Computer in the same circumstances as convictions are recorded. This has ensured that the PNC holds details of relevant matters for disclosure on criminal record certificates.

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

28. This section updated the references to various criminal record certificates in the Data Protection Act 1998. This has allowed for the commencement of section 56 of the Data Protection Act 1998. This makes 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'), unless it is required or authorised by law or in the particular circumstances it is justified as being in the public interest.

## **PART 5 - SAFEGUARDING VULNERABLE GROUPS**

### **Chapter 3**

#### **Introduction**

1. Chapter 3 of Part 5 established a new organisation, to be known as the Disclosure and Barring Service (“DBS”), which replaced and combined the functions of the ISA and the CRB.

#### **Implementation**

2. By virtue of section 120(5), sections 88 to 91 came into force on 1 May 2012 (Royal Assent).
3. The Protection of Freedoms Act 2012 )Commencement No. 4) Order 2012/2521 brought into force section 87(1) to (2) and (3) in respect of paragraphs 1 to 11 and 13 to 20 of Schedule 8 on 15 October 2012, and the remainder of section 87(3) on 1 December 2012.

#### **The following secondary legislation supports the Act:**

4. Ch3, Part Five, Schedule 8:
  - The Protection of Freedoms Act 2012 (Commencement No. 4) Order 2012/2521, made 3 October 2012.
  - Police Act 1997 (Criminal Records) (Jersey) (Amendment) Order 2012/2591, made 17 October 2012 (not yet in force). Extends certain provisions of PoFA to Jersey, subject to modification.
  - Police Act 1997 (Criminal Records) (Guernsey) (Amendment) Order 2012/1762, made 10 July 2012. Extends certain provisions of PoFA to Guernsey, subject to modification.
  - Police Act 1997 (Criminal Records) (Isle of Man) (Amendment) Order 2012/2598, made 17 October 2012, Extends certain provisions of PoFA to the Isle of Man, subject to modification.
  - Disclosure and Barring Service (Core Functions) Order 2012/2522, made 3 October 2012, laid on 5 October 2012, coming into force 1 December 2012. Specifies the core functions of the DBS.
  - Protection of Freedoms Act 2012 (Disclosure and Barring Service Transfer of Functions) Order 2012/3006, made 29 November 2012, coming into force 1 December 2012. Transfers functions of the ISA, and functions of the Secretary of State exercised by the CRB, to the DBS. Dissolves the ISA.

- Protection of Freedoms Act 2012 (Consequential Amendments) No. 2 Order 2013/1196, made 20 May 2013, laid 23 May 2013, coming into force 17 June 2013. Replaces references to Secretary of State with DBS in the Police Act 1997 (Criminal Records) (Fees) Order 2004.
- Disclosure and Barring Service (Core Functions) (Amendment) Order 2014/238, MADE 5 February 2014, laid 13 February 2014, coming into force 10 March 2014. Removes certain functions from SI 2012/2522 to allow DBS to delegate these functions.

## **Preliminary Assessment of the Act**

### **Section 87: Formation and constitution of DBS**

5. *Subsections (1) and (2)* establish a new body, called the Disclosure and Barring Service (“DBS”). The DBS is intended to combine the 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**

6. *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.
7. *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.
8. *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.

9. The Disclosure and Barring Service (Core Functions) Order 2012/2522 specifies the core functions of the Disclosure and Barring Service (“DBS”) under Part 5 of the Police Act 1997 (“the 1997 Act”). Functions which are core functions of the DBS cannot be delegated to a person who is neither an appointed member nor a member of staff of the DBS (under paragraph 7 of Schedule 8 to the Protection of Freedoms Act). The functions specified in article 2 of this Order are the functions under Part 5 of the 1997 Act which cannot be delegated. These functions include decision-making about what information needs to be submitted in an application for a certificate, whether a certificate was correctly applied for, setting conditions for the use of the electronic service and the up-date service, indentifying the chief officer of police for the purposes of providing information in relation to an application, dealing with disputes over certificates, verifying the identity of applicants, receiving police information and paying fees for that information and maintaining the register of persons able to countersign applications, including dealing with suspension and cancellation of that registration.
10. The Disclosure and Barring Service (Core Functions) (Amendment) Order 2014/238 amends the Disclosure and Barring Service (Core Functions) Order 2012 to remove various functions relating to the issue of a criminal conviction certificate (within the meaning of section 112 of the Police Act 1997) from that Order, so that they are no longer core functions within the meaning of paragraph 8 of Schedule 8 to the Protection of Freedoms Act. This allows those functions to be delegated by the Disclosure and Barring Service under paragraph 7 of Schedule 8 to the Protection of Freedoms Act.
11. *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.
12. *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.



13. *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.
14. *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.
15. The Secretary of State has issued three ministerial direction letters directing the DBS to delegate functions under paragraph 6 of Schedule 7, relating to the provision of basic checks by Disclosure Scotland.
16. The Chair of the Board was appointed as Chair from 1 December 2012 until 30<sup>th</sup> November 2017. Seven non-executive directors were appointed on 1 December 2012 when the Board formally assumed its responsibilities. The DBS Board make-up is available on [www.gov.uk](http://www.gov.uk).
17. The first Chief Executive was appointed by the Secretary of State on 1 December 2012 and resigned in 2015. The DBS Board appointed an acting Chief Executive in March 2016 and the new Chief Executive was appointed in June 2016 following consultation with the Secretary of State.
18. The Chief Executive is the Accounting Officer. DBS business plans, annual report and accounts and strategic plans are published on [www.gov.uk](http://www.gov.uk) and laid in Parliament by Written Ministerial Statement.

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

19. *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 Safeguarding Vulnerable Groups Act (the CRB's

functions in connection with the safeguarding of vulnerable groups); and the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (SI 2007/1351) (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**

20. *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.

21. All the ISA's functions under the Safeguarding Vulnerable Groups Act 2006, the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007, the Safeguarding Vulnerable Groups Act 2006 (Transitional Provisions) Order 2008 and the Safeguarding Vulnerable Groups (Transitional Provisions) Order (Northern Ireland) 2008, with the exception of the obligation to establish the barred lists, were transferred to the DBS under article 2 of the Protection of Freedoms Act (Disclosure and Barring Service Transfer of Functions) Order 2012/3006. Part 3 of this Order transferred to the DBS functions of the Secretary of State exercised by the CRB under Part 5 of the Police Act 1997. Having transferred the ISA's functions to the DBS, Part 5 of this Order dissolved the ISA under section 88(3) of the Protection of Freedoms Act.

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

22. 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.

23. *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 after being made.

### **Section 91: Tax in connection with transfer schemes**

24. 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.

## **PART 5 - SAFEGUARDING VULNERABLE GROUPS**

### **Chapter 4**

#### **Introduction:**

1. 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.
2. The chapter fulfils a 2010 commitment by the coalition government to “change the law so that historical convictions for consensual gay sex with over 16s...will not show up on criminal records checks”.

#### **Implementation**

3. SI 2012/2234 brought into force all provisions of Chapter 4 (sections 92 to 101) on 1 October 2012.

#### **Secondary legislation**

4. The Protection of Freedoms Act 2012 (Commencement No. 3) Order 2012/2234, made 28 August 2012, commenced all provisions of Chapter 4.
5. The Protection of Freedoms Act 2012 (Relevant Official Records) Order 2012/2279 was made on 4 September 2012, laid 6 September 2012 and came into force on 1 October 2012. Made under s.95(5) and (6), this Order prescribes which records of convictions and cautions are relevant official records (in addition to the names database) and prescribes the relevant data controller in relation to those relevant records. It also makes provision for certain records to be annotated rather than deleted.

#### **Preliminary assessment of the Act**

6. 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.

7. This fulfils a 2010 commitment by the coalition government to “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”. The legislation goes further than the commitment - convictions would not be treated as spent, but would be disregarded (deleted or where not possible annotated). Spent convictions would appear on enhanced disclosures, whereas disregarded offences do not.
8. The initial scope of the disregard scheme was England and Wales. Later section 168 of the Policing and Crime Act 2017 mirrored the scheme in Northern Ireland, with the consent of the Northern Ireland Assembly, taking into account regional differences, by inserting a new Chapter 5 into Part V of the Protection of Freedoms Act. Chapter 5 is not yet in force. Lord Lexden stated in the Lords “gay people in Northern Ireland felt that their part of our country should not be excluded from such an important measure of belated justice” (Hansard, 12 December 2017). The Scottish government have announced their intention to introduce a similar scheme in Scotland.

### **Section 92 Power of Secretary of State to disregard convictions or cautions**

9. Subsections (1) to (4) specify the offences for which a conviction or caution can be disregarded and the conditions which must be met. The offences are primarily sections 12 and 13 of the Sexual Offences Act 1956, but also include equivalent offences under earlier legislation. The three conditions to be met before a conviction or caution for an offence can be disregarded are:
  - The other person involved in the conduct consented to it;
  - The other person was aged 16 or over; and
  - Any such activity now would not be an offence under section 71 of the Sexual Offences Act 2003 (sexual activity in a public lavatory).
10. Where the relevant conditions are met the Secretary of State will give notice to the applicant and 14 days later the conviction or caution will become a disregarded conviction or caution (subsections (2) and (4)).

11. After introduction of the disregard scheme there were calls to extend the scope of the scheme to other offences, in particular to include section 32 of the Sexual Offences Act 1956 (soliciting). This later resulted in the introduction of section 166 of the Policing and Crime Act 2017 which provides a mechanism to extend the disregard scheme to additional abolished offences by means of statutory instrument (this power has not yet been used).
12. Extending the scope requires careful analysis to ensure a disregard does not result in the deletion of records of activity which would still be a crime today. Section 32 of the Sexual Offences Act 1956 was used to cover a wide range of activity and we need to establish a mechanism to resolve which cases would be eligible and which would not. To date ten applications for section 32 offences have been rejected as out of scope, most of which would also be rejected for other reasons, primarily sexual activity in a public lavatory.
13. The Fact Sheet for the legislation estimated there to be 50,000 convictions and cautions recorded on the Police National Computer for Section 12 and 13 offences, and an estimated 16,000 related to behaviour that was decriminalised. The actual number of applicants is significantly lower:

**Chapter 4 disregards: 4 April 2017**

Year of application	Applicants	Cases	Cases Accepted	Cases Rejected	Invalid cases	Cases in progress
2012	35	38	14	7	17	0
2013	83	103	28	23	52	0
2014	50	71	16	14	41	0
2015	54	76	22	13	41	0
2016	75	113	31	28	49	5
2017	31	49	2	6	21	20
TOTAL	328	450	113	91	221	25

### Accepted cases

Year of application	Section 12 (buggery)	Section 13 (gross indecency)	Military equivalents	Older legislation	TOTAL
2012	1	13	0	0	14
2013	1	27	0	0	28
2014	2	13	1	0	16
2015	0	20	2	0	22
2016	3	28	0	0	31
2017	1	1	0	0	2
Total	8	102	3	0	113

### Rejected and invalid cases

Year of application	Valid applications					Invalid applications		
	Public lavatory	Non consensual	Under age	No info found	Total	Not eligible	Unrelated	Total
2012	7	0	0	0	7	3	14	17
2013	18	4	1	0	23	11	41	52
2014	7	2	0	5	14	6	35	41
2015	4	2	2	5	13	2	39	41
2016	19	0	3	6	28	7	42	49
2017	5	0	0	1	6	20	1	21
Total	60	8	6	17	91	49	172	221

14. Some cases may be rejected for more than one reason, in which case only one reason is counted in the statistics.

### Section 93 Applications to the Secretary of State

15. This section establishes the process for applying for a disregard.
16. The process for applying involves providing proof of identity and of current address as well as details of the conviction, in particular the time when and the place where the conviction was made or the caution given and, for a conviction, the case number, and such other information as the Secretary of State may require.
17. At times the information provided has been unclear with, for example, some applicants being uncertain of the decade an offence has taken place, but in practice, with the name and date of birth, the relevant records have been found.
18. For a small minority of cases (17) no police records were found, even when the applicant has provided specific details. Most of these were described by the applicant as cautions, however we believe at the time the police gave the person an informal warning (as distinct from a caution) and no information was recorded, but the applicant misunderstood this as a caution. As there is no information to disregard, the application is rejected, but this should not affect the applicant as there are no records to appear on criminal record certificates.

#### **Section 94 Procedure for decisions by the Secretary of State**

19. 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.
20. *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.
21. Subsections (3) and (4) provide that the Secretary of State must record the decision with reasons and give notice to the applicant.

#### **Section 95 Effect of disregard on police and other records**

22. This section provides that where a conviction or caution is disregarded, the Secretary of State must direct the relevant data controller to delete or annotate the details of the disregarded caution or conviction from all official records.



Generally records are deleted, but there are cases where this is not possible, for example where the records are on microfiche along with other information which cannot be deleted. In this case the microfiche is annotated to the effect that the information in question must be treated as if deleted.

23. In most cases the data controller will be the chief officer of police of the force which investigated the offence.

24. Subsections (5) and (6) provide that other relevant official records and data controllers may be prescribed by order subject to the negative resolution procedure. The Protection of Freedoms Act (Relevant Official Records) Order 2012/2279 was made using these powers.

25. The disregard process has worked well, with data controllers responding to requests for information, and requests to delete records. The range of data controllers, covering local police forces, military equivalents and the courts, has covered all applications received and no extensions or modifications to the list of data controllers is required.

### **Section 96 Effect of disregard for disclosure and other purposes**

26. *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).

27. *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).

28. *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.

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

30. *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.

31. We are not aware of any cases where disregarded cautions or convictions have been improperly treated.

### **Section 97 Saving for Royal pardons etc.**

32. This section preserves the power of Her Majesty, under the Royal prerogative, to issue a pardon, commute a sentence or quash a conviction.

33. After the introduction of the disregard scheme there were campaigns, from within and outside parliament, to introduce a pardon for those convicted of gay sexual offences. This later resulted in the introduction of sections 164 and 165 of the Policing and Crime Act 2017 which provide a pardon for cautions or convictions which have been or are in the future disregarded as well as a posthumous pardon for those who were eligible for a disregard but died before the provision came into force.

### **Section 98 Section 96: supplementary**

34. This section defines terms used in section 96.

### **Section 99 Appeal against refusal to disregard convictions and cautions**

35. 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.

### **Section 100 Advisers**

36. This section 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. The decision on the application will rest with the Secretary of State, who can accept, or not, the advice provided.

37. An advisory panel of three independent experts was set up but was stepped down after their three year contract period as there were insufficient cases needing referral. The role was taken over by Home Office Legal Advisers. There has only been one case where legal advisers provided advice to policy colleagues which informed their advice to the Secretary of State.

#### **Section 101 Interpretation: Chapter 4**

38. This section defines various terms used in this chapter. In particular, by virtue of this section, eligible offences under section 92(1) include equivalent military offences, as well as inchoate offences such as attempting to commit or aiding the commission of the relevant offence.

39. There have been three successful applications for equivalent military offences and a similar number of rejected cases. Rejected cases were for non-consensual activity or for sexual activity in a public lavatory. The process is similar to that for non-military offences, with data controllers identified for the military services.

## **PART 6 – FREEDOM OF INFORMATION AND DATA PROTECTION**

### **Introduction:**

1. The Programme for Government (section 3: civil liberties and section 16: government transparency) stated 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*”.
2. 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.
3. 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.

4. 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<sup>29</sup>. Government datasets are available at: [www.data.gov.uk](http://www.data.gov.uk).
5. The Government's proposals for extending the scope of the FOIA were announced on 7 January 2011.
6. First, part 6 amends the FOIA to make provision for the re-use of datasets by public authorities subject to that Act.
7. Secondly, it amends 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.
8. Thirdly, it extends to Northern Ireland amendments made to the FOIA by the Constitutional Reform and Governance Act 2010.
9. Finally, it amends 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.

### **Implementation**

10. The amendments relating to datasets came into force on 31 July 2013 or 1 September 2013. The amendments relating to publicly owned companies came into force on 1 September 2013. The extension to Northern Ireland came into force on 1 July 2012. The amendments relating to the Information Commissioner came into force on 16 March 2015. Those relating to the role of the Secretary of State in relation to the exercise of certain functions by the Information Commissioner came into force on 1 September 2013.

### **Preliminary assessment of the Act**

11. The changes relating to freedom of information and data protection have not given rise to any issues or concerns.

---

<sup>29</sup> [Letter to Government departments on opening up data | Number10.gov.uk](#)

## **PART 7 – MISCELLANEOUS AND GENERAL**

### **Part 7 section 109 and 110 - Trafficking people for exploitation**

#### **Introduction**

1. 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)<sup>30</sup>. 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.
2. Part 7 made two principal changes to existing criminal offences on human trafficking in order to comply with Directive 2011/36/EU of the European Parliament and of the Council on preventing and combating trafficking in human beings and protecting its victims.
3. It expanded 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 traffic a person into, within, or out of the United Kingdom for the purposes of exploitation.
4. It also made it an offence for a UK national to traffic 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.
5. It amended 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.

#### **Implementation:**

6. The provisions of sections 109 and 110 were not commenced and were subsequently repealed by The Modern Slavery Act 2015

#### **Preliminary assessment of the Act**

---

<sup>30</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:EN:PDF>

7. As the legislation has been repealed, we should look at the rationale behind the Modern Slavery Act to explain that the Act consolidates the previously existing legislation, helping to simplify and bring into one place the various measures that existed previously.
8. The Modern Slavery Act gives law enforcement the tools to fight modern slavery, ensure perpetrators can receive suitably severe punishments for these appalling crimes and enhance support and protection for victims. It received Royal Assent on Thursday 26 March 2015. The Act:
  - Consolidates and simplifies existing offences into a single Act.
  - Ensures that perpetrators receive suitably severe punishments for modern slavery crimes (including life sentences).
  - Enhances the court's ability to put restrictions on individuals where it's necessary to protect people from the harm caused by modern slavery offences.
  - Creates an independent anti-slavery commissioner to improve and better coordinate the response to modern slavery.
  - Introduces a defence for victims of slavery and trafficking.
  - Places a duty on the secretary of state to produce statutory guidance on victim identification and victim services.
  - Enables the secretary of state to make regulations relating to the identification of and support for victims.
  - Makes provision for independent child trafficking advocates.
  - Introduces a new reparation order to encourage the courts to compensate victims where assets are confiscated from perpetrators.
  - Enables law enforcement to stop boats where slaves are suspected of being held or trafficked.
  - Requires businesses over a certain size to disclose each year what action they have taken to ensure there is no modern slavery in their business or supply chains.

## **PART 7 – MISCELLANEOUS AND GENERAL**

### **Part 7 Section 111 and Section 112 regarding stalking**

1. Section 111(1) inserted new section 2A into the Protection from Harassment Act 1997 (“the 1997 Act”) to create a new offence of stalking in England and Wales. A person is guilty of committing the offence if that person pursues a course of conduct in breach of the prohibition on harassment in section 1(1) of the 1997 Act and the course of conduct amounts to stalking.
2. Section 2A(2) of the 1997 Act 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.
3. Section 2A(3) of the 1997 Act provides a (non-exhaustive) list of examples of behaviour that may be associated with stalking, such as ‘following a person’ and ‘watching or spying on a person’.
4. 2A(4) of the 1997 Act provides that this is a summary only offence with a maximum penalty of six months imprisonment or an unlimited fine.
5. Section 111(2) inserted new section 4A into the 1997 Act to create a new offence of stalking involving fear of violence or serious alarm or distress. A person (A) is guilty of committing the offence where that person pursues a course of conduct amounting to stalking and either:
  - a. causes another to fear, on at least two occasions, that violence will be used against them or
  - b. causes another serious alarm or distress which has a substantial adverse effect on their usual day-to-day activities and knows or ought to know that their course of conduct will have such an effect on the victim.
6. Sections 4A(2) provides that A must know or ought to know that their conduct will cause the other person to fear that violence will be used against them or will cause the other person serious alarm or distress, and section 4A(3) provides that “ought to know” means 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.
7. 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 an unlimited fine 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**

8. Section 112 inserted new section 2B into the 1997 Act to create a new power of entry in England and Wales in relation to the section 2A stalking offence. The power allows the police to apply to the magistrates' court for a warrant to allow them to enter and search premises.
9. In order to grant such a warrant, the magistrates' court must be satisfied that:
  - a section 2A stalking offence has been or is being committed;
  - there is material on the premises which is likely to be of 'substantial value' to the investigation of the offence, and that that material is both likely to be admissible as evidence in relation to any trial for the offence and does not include/consist of items subject to legal privilege, excluded material or special procure material (as defined in sections 10, 11, and 14 of the Police and Criminal Evidence Act 1984), and either
  - the police will not be able to gain entry to the premises without a warrant, or
  - the purpose of a search may be 'frustrated or seriously prejudiced' unless the police can secure immediate entry to the premises when they arrive.Where such a warrant is granted, the police may seize and retain anything for which the search was authorised. In addition in exercising this power the police may use reasonable force if necessary.

### **Implementation**

10. The stalking offences were introduced following a public consultation in 2011. To support the consultation, the Home Office held four regional road shows to increase awareness of stalking and to gain feedback on the consultation from specialists, frontline staff and victims of stalking. The consultation response was published in July 2012.
11. The purpose of introducing the offences was to: highlight stalking as a specific behaviour (as distinct from other types of harassment, harassment already being an offence under the Protection from Harassment Act 1997); close a legislative gap so that where a perpetrator's conduct does not cause the victim to fear violence but does cause them serious alarm or distress this may still be an either way offence and; help raise awareness of stalking. The offences came into force on 25 November 2012.
12. The new power of entry was introduced in response to the consultation to support the investigation of, and evidence gathering for, cases involving stalking.
13. Ahead of the offences and power of entry coming into force, on 16 October 2012 the Home Office issued a circular (018/2012) providing an overview of the new measures to key stakeholders, including Police and Crime Commissioners, the then Association of Chief Police Officers, the Association Of Magisterial Officers, Justices Clerks Society, and the Judicial Studies Board.

14. The Police and Crime Act 2017 raised the maximum sentence for the section 4A offence from five years to ten years.

### **Guidance and training**

15. In January 2013 the College of Policing issued a [briefing note](#) for Amendments to the Protection from Harassment Act 1997 and the CPS has also issued [guidance](#) for prosecutors. Following this, in September 2014, the Crown Prosecution Service (CPS) and the then Association of Chief Police Officers (ACPO) launched a new [protocol](#) to help embed the new offences and ensure consistency of approach in tackling stalking. The protocol advises police and prosecutors on:

- how to ensure that in every case the victim has the opportunity to provide a Victim Personal Statement to court and is able to read this out personally should they wish;
- fully investigating the reasons behind any victim withdrawing a complaint, ensuring it is not the result of pressure from others and;
- ensuring that victims are consulted on issues such as bail and restraining orders.

16. In addition, in April 2014 the CPS launched a specific e-learning module on stalking which focused on victim support, working with the police and ensuring a strong case is built from the start. As of December 2016, over 1,600 CPS staff had completed this training. In October 2014 the CPS issued follow-up training material on the stalking offences to enable face-to-face training and review and embed the learning from the e-learning. The learner's knowledge and understanding of the law and policy is tested through a number of questions.

### **Other Reviews**

#### **HMIC/ HMCPS inspection**

17. In July 2017, Her Majesty's Inspectorate of Constabulary (HMIC) and Her Majesty's Crown Prosecution Service Inspectorate (HMCPSI) published the findings of a joint inspection into the police and CPS response to stalking and harassment. The report found that, while there are examples of individual good practice, overall understanding and awareness of these crimes is low, and, of 112 cases they assessed from six areas, none had been dealt with well overall.

18. The report makes 22 recommendations for the Home Office, the police, CPS, and College of Policing, including regarding the legal definition of 'stalking', reviewing the police approach to risk assessment, and guidance and training for the police and prosecutors. The Government is working with the police, CPS and others to address the report's findings.

House of Commons Report: *Stalking – The Case for Extending the Maximum Penalty*

19. This report was published in April 2016 by Alex Chalk MP and Richard Graham MP and reviewed the prevalence of stalking, drawing on recent cases, and the case for increasing the maximum sentence. The report's key findings was that as stalking can occur over a long period of time, it cannot always be properly addressed by short prison sentences, and the report therefore recommended that the maximum sentence should be increased to allow judges greater flexibility.

Northern Ireland Assembly: *Legislative Position on Stalking and Relevant Statistics in the UK and the Republic of Ireland*

20. In January 2017, the Northern Ireland Assembly published a report into the different legislative approaches to tackling stalking. This included looking at the legislative approach on stalking in England and Wales.

**Preliminary assessment of the Act**

21. The stalking offences are being used by the police and prosecutors. The statistics show that:

- In the year to June 2016, the police recorded 4,168 stalking offences, an increase of 32% since the previous year (3,166). Most of the rise in police recorded crime is thought to be due to improved crime recording practices and processes leading to a greater proportion of reports of crime being recorded in the last year than the previous one and a greater willingness of victims to report crimes to the police.
- As of 1 April 2014, for the purposes of police crime data, stalking as a specific legal offence became recorded in a separate category.
- In 2015-16 1,102 prosecutions were commenced under the new stalking offences. This is similar to 2014-15 when 1,103 prosecutions commenced and follows a rise from earlier years (743 prosecutions commenced in 13-14, and 67 offences charged in 12-13).

Professional awareness

22. The new stalking offences highlighted stalking as a specific behaviour as distinct from harassment more generally. However, there are still concerns regarding police and prosecutors' ability to differentiate between the types of offences.

23. Whilst 'stalking' is not defined in the legislation, Section 2A(3) lists a number of examples of behaviours associated with stalking. The list is not an exhaustive one but gives an indication of the types of behaviour that may be displayed.

24. In addition to the training and guidance issued to support the introduction of the new offence, the CPS recently set up a working group with Paladin (National Stalking Advocacy Service), the Suzy Lamplugh Trust (National Stalking Helpline), the Home Office and the Ministry of Justice to consider what additional training can be offered to CPS prosecutors so they are better able to differentiate between stalking and harassment offences; this work is on-going.
25. In addition, the National Policing Lead chairs a regular group to drive a more effective response. The Home Office is a member of the Group. The CPS and police are revising the joint protocol on stalking to ensure that it better supports police officers and prosecutors to build robust cases which fully consider the impact of this crime on the victim. A checklist to prompt police officers about useful areas of evidence will be included. Additionally, the eLearning module on Stalking and Harassment together with a module on Restraining orders has been refreshed and all prosecutors will need to complete this during 2018.
26. The Government will continue to keep the stalking offences under review, including as part of a range of work following the HMIC/HMCPSP stalking and harassment inspection.

#### Wider work

27. There is a range of wider work under way to tackle stalking:
- Policy on stalking forms part of the cross-Government 2016-20 Violence Against Women and Girls (VAWG) strategy which is supported by £100 million of funding. The strategy is supported by a National Statement of Expectations (NSE) was published in December 2016 and sets out what local areas need to do to prevent offending, support victims and will encourage organisations to work with local commissioners to disseminate the NSE and support implementation of best practice.
  - Since 2010, the Home Office has provided funding to support the National Stalking Helpline. In addition, the VAWG Transformation Fund's £17 million will provide additional support to victims, including those being stalked.
  - From 5 December 2015 to 29 February 2016, the Government ran a public consultation on introducing a new stalking protection order. In December 2016, the Government published the findings of its consultation which demonstrated support for the introduction of a new civil stalking protection order to support victims of stalking and address the perpetrator's behaviours at an early stage.
  - The Government subsequently published its consultation response which confirmed an order would be introduced. The order will:
    - be available on application from the police to a magistrates' court;
    - allow for both restrictions and positive requirements to be imposed, depending on the circumstances of the case; and

- incur a criminal penalty for breach (max. sentence 5 years' imprisonment) to encourage perpetrators to comply with the order's conditions and ensure breaches are appropriately punished.
- Primary legislation is required to introduce the order and will be taken forward as soon as Parliamentary time allows.

## **PART 7 – MISCELLANEOUS AND GENERAL**

1. Part 7 Section 113 - repealed the unimplemented section 43 of the Criminal Justice Act 2003 (“the 2003 Act”), which made provision for certain fraud trials to be conducted without a jury.
2. Section 43 would have allowed the prosecution to apply in certain circumstances for a serious or complex fraud trial to proceed in the absence of a jury. The judge was to have power to order the trial to be so conducted if satisfied that the length/complexity of the case was likely to make the trial so burdensome upon the jury that the interests of justice required serious consideration to be given to conducting it without a jury.
3. Section 43 was opposed by the Conservatives and the Liberal Democrats, and in order to secure its passage its implementation was made subject to a restriction (in section 330(5)(b)) whereby an order bringing section 43 into force would have to go through the affirmative resolution procedure.
4. An unsuccessful attempt to bring section 43 of the 2003 Act into force was made in November 2005, when a draft commencement order was considered in standing committee in the House of Commons, but the Government withdrew it before it was due to be debated in the House of Lords. 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). No further steps were taken and section 43 remained unimplemented.
5. When the Coalition Government was formed in 2010, its Programme for Government (section 3: civil liberties) included a commitment to “*protect historic freedoms through the defence of trial by jury*”. The then Government took the view that repealing section 43 would demonstrate that commitment, and that the Protection of Freedoms Bill was an appropriate vehicle for that repeal.

## **PART 7 – MISCELLANEOUS AND GENERAL**

### **Part 7: section 114**

#### **Introduction**

1. The text in the final paragraph of the background to the Explanatory Note accurately reflects the objective of section 114 of the Protection of Freedoms Act in removing the restriction on the times when a marriage or civil partnership may take place in England or Wales and the associated offences. Therefore, Section 114 allows a marriage or civil partnership to take place at any time of the day or night.

#### **Implementation**

2. The provisions of section 114 were brought into operation on 1 October 2012 by virtue of Article 3(m) of the Protection of Freedoms Act (Commencement Number 3) Order (SI 2012/2234).
3. There was no delegated legislation required for the implementation of section 114. Registration officers and local authorities who are responsible for the delivery of civil registration services were informed of the change by means of a Circular issued on the 6 July 2012 and a subsequent Question and Answer briefing. Guidance documents for registration officers and authorised persons, who officiate at religious marriage ceremonies (other than in the Church of England/Church in Wales) were revised to reflect the removal of the hours of restriction on marriage. This advised that the acceptance of marriage appointments outside of normal hours was permissible with no obligation on local authorities or religious bodies to provide such a service. A public announcement of the change was made via a news announcement published on Gov.uk by the Home Office on 1 October 2012.

#### **Preliminary assessment of the Act**

4. The purpose of section 114 of the Protection of Freedoms Act was fully met through the resulting amendment to the Marriage Act 1949 and the Civil Partnership Act 2004 (and a consequential amendment to the Marriage (Registrar General's Licence) Act 1970). While customer demand for ceremonies outside the previously restricted hours has been low, some couples have taken advantage of the freedoms. This was particularly evident with ceremonies being held at midnight on the commencement of the Marriage (Same Sex Couples) Act 2013. Although the impact of this change has been low it nevertheless continues to provide couples with the potential for greater choice of the time of their marriage or civil partnership.

CCS0218087168

978-1-5286-0235-8