ANNUAL REPORT 2014

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Alastair R MacGregor QC

November 2014

Office of the Biometrics Commissioner

ANNUAL REPORT 2014

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Presented to Parliament pursuant to Section 21(4)(b) of the Protection of Freedoms Act 2012

December 2014

© Commissioner for the Retention and Use of Biometric Material copyright 2014.

The text of this document (this excludes, where present, the Royal Arms and all departmental or agency logos) may be reproduced free of charge in any format or medium provided that it is reproduced accurately and not in a misleading context.

The material must be acknowledged as **Commissioner for the Retention and Use of Biometric Material** copyright and the document title specified. Where third party material has been identified, permission from the respective copyright holder must be sought.

Any enquiries related to this publication should be sent to us at Enquiries@BiometricsCommissioner.gsi.gov.uk.

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

Print ISBN 9781474113311
Web ISBN 9781474113328

ID 09121405 12/14

Printed on paper containing 75% recycled fibre content minimum

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

FOREWORD

This is my first Report as the Commissioner for the Retention and Use of Biometric Material. I was appointed to that role by the Home Secretary on 4 March 2013 under Section 20 of the Protection of Freedoms Act 2012 ('PoFA'). PoFA established a new regime to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints. It also laid down new rules about the retention of such material on national security grounds by police forces anywhere in the United Kingdom.

The structure of this Report is as follows.

In **Section 1** I explain the legislative background to, and the nature and scope of, the retention regime for biometric material which was established by PoFA. I also summarise the steps that were taken to implement that new regime and my statutory responsibilities as Biometrics Commissioner.

In **Section 2** I deal with the discharge of my responsibilities as regards applications by the police for consent to the extended retention of DNA profiles and/or fingerprints from individuals who have been arrested for, but not charged with, 'qualifying' offences. In particular I deal with:

- the relevant provisions of the legislation, the consultation exercise that I conducted before the new regime took effect, and the principles that I apply when deciding such applications;
- the development and nature of the application and decision-making processes;
- the volume, grounds and upshot of the applications that have been received; and
- issues that have arisen in connection with such applications.

Matters of particular significance which are addressed in that section include:

- the definitional and other difficulties that arise as regards "*the conclusion of the investigation of the offence*" – a concept which is pivotal to the new retention regime but which is not defined in PoFA – and the way in which those difficulties have been approached (paragraphs 29-34);
- the number, nature and outcome of the applications for extended retention that were made between the commencement of the Act and 31 August 2014 (paragraphs 43-58);
- the difference between circumstances in which forensic evidence may be of value and circumstances in which some real purpose may be served by the retention of a particular arrestee's DNA profile or fingerprints (paragraphs 73-79);
- concerns that arise as regards:
    - the definition of 'qualifying' offences (paragraphs 89-90); and

- the taking and retention of biometric material from those who have been convicted of qualifying offences outside England and Wales (paragraphs 91-101); and
- the very small number of applications that have been received from forces other than the Metropolitan Police, possible reasons for this lack of engagement by other forces, the risks that arise in that connection, and the reasons why forces may consider that those risks are reasonable ones for them to run (paragraphs 102-113).

In **Section 3** I deal with the discharge of my responsibilities regarding national security determinations ('NSDs') and my general oversight function insofar as it relates to counter-terrorism matters. In particular I deal with:

- the relevant provisions of the legislation, the Statutory Guidance issued by the Home Secretary, the development and nature of the NSD process, and my own role in that process;
- the assessment of 'legacy' material, the rules that apply to 'new' material, and the past and future operation of the NSD process; and
- other matters relating to national security holdings of biometric material.

Matters of particular significance which are addressed in that section include:

- the provision of information to Chief Officers and myself (paragraphs 138-139, 142-145 and 150-152);
- concerns that have arisen about delays in the NSD process as regards material which has been collected since commencement (paragraph 161);
- the feasibility of the relevant authorities' completing by 31 October 2015 all the assessment and other work that is likely to be required by that date in connection with legacy material (paragraph 162);
- the handling of – and the governance arrangements that apply to – biometric material in the context of CT-related matters (paragraphs 166-169); and
- benefits to national security that have flowed from the introduction of the new retention regime (paragraphs 170-174).

In **Section 4** I deal with the destruction and/or deletion of DNA samples, DNA profiles and fingerprints to comply with the PoFA regime. In particular I deal with:

- the genesis and nature of the 'CPIA exception' whereby DNA samples may be retained beyond the normal destruction deadline if they are or may become disclosable in criminal proceedings;
- the destruction of legacy and new DNA samples by Forensic Science Providers and police forces, the compliance checks that have been and will be carried out in that connection, and the number of DNA samples that were being held under the CPIA exception on 31 August 2014;

- the deletion of legacy and new DNA profiles and fingerprints and the process of automatic deletion that is driven by the Police National Computer ('the PNC');
- the difficulties that have arisen as regards that automatic deletion process and as regards the destruction of hard copies of fingerprints; and
- the processes by which members of the public can request the early destruction or deletion of biometric material that is lawfully held by the police.

Matters of particular significance which are addressed in that section include:

- my concerns as regards:
    - the number of DNA samples – and particularly 'elimination' samples – that are being retained pursuant to the CPIA exception;
    - the likely duration of that retention; and
    - the obtaining of properly informed consent from individuals who provide biometric material for elimination purposes (paragraphs 185-192, 198-202 and 231);
- issues relating to the programming and operation of the PNC that have resulted in the deletion of biometric records which should have been retained and the retention of records which should have been deleted (paragraphs 207-222 and 232-233); and
- issues relating to the retention of hard copies of fingerprints, particularly in the National Archive and in police investigation case files (paragraphs 225-231 and 235).

In **Section 5** I deal with the use to which biometric material is being put. In particular I deal with the 'speculative searching' of DNA profiles and fingerprints and the international sharing of biometric material. Matters of particular significance which are addressed in that section include my concerns about issues relating to the effective operation of the speculative search process, especially as regards fingerprints (paragraphs 267-272).

In **Section 6** I deal with other matters relating to DNA samples, DNA profiles and fingerprints. In particular I deal with:

- DNA profiling problems and fibre contamination issues;
- fingerprint governance arrangements;
- enquiries and the provision of information; and
- the desirability of research.

Matters of particular significance which are addressed in that section include:

- the need for greater clarity as regards fingerprint governance arrangements, especially in view of the relationship between – and the work that is planned to – the police and immigration fingerprint databases (paragraphs 316-322);
- my concerns as regards the provision of information to members of the public about biometric material that may or may not be being retained by the police (paragraphs 325-328); and

- the need for proper research into the impact of the new biometric retention regime (paragraphs 332-335).

In **Section 7** I deal with important issues that arise as regards matters which relate to the retention and use of biometric material but which fall outwith the ambit of my responsibilities i.e. the creation of a searchable national police database of custody photographs and the application of facial recognition technology to that database (paragraphs 336-344).

In **Section 8** I deal with my Office's resources, accommodation and web presence.

I have not submitted a confidential annex to the national security (or any other) section of this Report as I do not feel that one is currently necessary. By section 21 of PoFA, however, the Home Secretary may (after consultation with me) exclude from publication any part of this Report if, in her opinion, the publication of that part would be contrary to the public interest or prejudicial to national security.

Alastair R MacGregor QC
Biometrics Commissioner **November 2014**

CONTENTS

1. INTRODUCTION

1.1 GENERALLY

1. The role of Commissioner for the Retention and Use of Biometric Material ('the Biometrics Commissioner') was established by the Protection of Freedoms Act 2012. That Act also established a new regime to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints. One of my responsibilities as Biometrics Commissioner is, in essence, to provide independent oversight of that new regime. I also have other, and more specific, 'casework' responsibilities as outlined below.

2. A DNA sample is usually taken from a person by way of a swab from the inside of the cheek. It contains the entirety of a person's genetic information. A DNA profile is a string of 10 – or, more recently, 16 – pairs of numbers and 2 letters (indicating gender) which is derived from a DNA sample and which can, like a fingerprint, be loaded to an electronic database. Although a DNA profile contains only very limited information about a person's genetic make-up, it is sufficient to allow that person to be identified if, for example, they leave their DNA at a crime scene.

3. No-one doubts the contribution that DNA and fingerprints, and the associated national databases, can and do make to the prevention and detection of crime. The much-debated question that arises, however, is how in that connection one strikes an appropriate balance between:

    - the public interest in the prevention and detection of crime; and
    - the individual's right to privacy, particularly in circumstances where that individual has never been convicted of an offence.

    Over the past 30 years (during which the police have been granted ever-widening powers to take DNA and fingerprints from those they suspect of involvement in criminal offences) Parliament has given a number of different answers to that question.

4. Between 1984 and 2001 the general rule was that fingerprints and DNA samples that were taken in connection with the investigation of an offence had to be destroyed as soon as practicable if the individual in question was not convicted of that offence. Between 2001 and 2013, however, the general rule was that, whether or not that individual was convicted of – or even (from 2003) charged with – that offence, all such prints and samples could be retained indefinitely.

5. In 2008 the Grand Chamber of the European Court of Human Rights ('ECtHR') gave its decision in the case of *S and Marper v United Kingdom*.[1] In that case the applicants, one of whom had been 11 years old when he was arrested and neither of whom had been

[1] (2008) 48 EHRR 1169

convicted of an offence, complained that their DNA samples, DNA profiles and fingerprints were nonetheless subject to indefinite retention. The ECtHR noted that the United Kingdom was the only Council of Europe member state expressly to permit (in England, Wales and Northern Ireland) "*the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued*" and that even in Scotland a much less draconian regime applied.[2] It concluded that the "*blanket and indiscriminate nature*" of the retention powers for DNA samples, DNA profiles and fingerprints failed to strike "*a fair balance between the competing public and private interests*".[3]

6. In response to that decision Parliament passed the Crime and Security Act 2010 which, among other things, would have allowed for:

- the retention for six years of fingerprints and DNA profiles of people arrested for, but not convicted of, recordable offences; and
- the extended retention of fingerprints and DNA profiles on national security grounds.

Following the General Election in 2010, however, the relevant provisions of that Act were not brought into force and they were subsequently repealed by the Protection of Freedoms Act 2012 ('PoFA').[4]

1.2 THE NEW BIOMETRIC REGIME

7. Put shortly, what Parliament in essence decided when it introduced the new PoFA regime was:

- first, that as regards the retention of biometric material by the police, much more restrictive rules should apply to the retention of DNA samples than should apply to the retention of DNA profiles and fingerprints; and
- second, that the rules applying to DNA profiles and fingerprints should draw a clear distinction between those who have been convicted of offences and those who have not.

That new regime – which was largely introduced by way of amendments to the Police and Criminal Evidence Act 1984 ('PACE') – can be summarised as follows.

DNA SAMPLES

8. As regards DNA samples, the general rule provided for in PoFA is that any DNA sample that is taken in connection with the investigation of an offence must be destroyed as soon as a

[2] See e.g. paragraphs 47 and paragraphs 36 and 109.

[3] See e.g. paragraphs 119 and 125.

[4] See Part 1 of Schedule 10.

DNA profile has been derived from it and in any event within six months of the date it was taken. That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.

PROFILES AND FINGERPRINTS[5]

9. As regards DNA profiles and fingerprints – which contain much less information about the people from whom they are taken – the general rule provided for in PoFA is:

- that they can continue to be kept indefinitely if the individual in question has been or is convicted of a recordable offence; but
- that in almost all other circumstances they must be deleted from the national databases at the conclusion of the relevant investigation or proceedings.

In this context a 'recordable offence' is, broadly speaking, any offence which is punishable with imprisonment[6] and, importantly, an individual is treated as 'convicted of an offence' not only if they have been found guilty of it by a court but also if, having admitted it, they have been issued with a formal caution (or, if under 18, a formal warning or reprimand) in respect of it.[7]

10. There are, however, a number of exceptions to that general rule, particularly as regards:

- its application to those who commit offences when they are under the age of 18 and/or to whom a Penalty Notice for Disorder (a PND) is issued; and
- where someone is arrested for, albeit not convicted of, a 'qualifying' offence.

A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.[8]

11. Put briefly, in those latter circumstances (i.e. where the relevant offence is a 'qualifying offence') DNA profiles and fingerprints can be retained for longer periods than would otherwise be the case in the absence of a conviction. In particular:

- if a person without previous convictions is charged with a qualifying offence, then, even if they are not convicted of that offence, their DNA profile and fingerprints can be retained for three years from the date of their arrest; and
- if a person without previous convictions is arrested for, but not charged with, a qualifying offence, the police can apply to the Biometrics Commissioner for consent to the extended retention of that person's DNA profile and/or fingerprints – and, if

[5] By section 65(1) of PACE: *'"fingerprints", in relation to any person, means a record (in any form and produced by any method) of the skin pattern and other physical characteristics or features of (a) any of that person's fingers; or (b) either of his palms.'*

[6] See section 118 of PACE.

[7] See (new) section 65B of PACE and section 65 of the Crime and Disorder Act 1998.

[8] See section 65A(2) of PACE.

the Commissioner accedes to that application, the profile and fingerprints can again be retained for three years from the date that that person was arrested.

In both those cases, moreover, that 3-year retention period can later be extended for a further two years by order of a District Judge.

12. Finally, the new regime also allows for the extended retention of DNA profiles and fingerprints on national security grounds if a National Security Determination ('an NSD') is made by the relevant Chief Officer.

13. The retention regime established by PoFA in respect of DNA profiles and fingerprints taken under PACE can be summarised in schematic form as follows.

CONVICTIONS

Person	Type of offence	Time period
Adults	**Any recordable offence (includes cautions)**	**Indefinite**
Under 18 years	**Qualifying offence (includes cautions, warnings and reprimands)**	**Indefinite**
Under 18 years	**Minor offences (includes cautions, warnings and reprimands)**	
	1st conviction – sentence under 5 years	**Length of sentence + 5 years**
	1st conviction – sentence over 5 years	**Indefinite**
	2nd conviction	**Indefinite**

NON CONVICTIONS

Alleged offence	Police action	Time period
All Offences	**Retention allowed until the conclusion of the relevant investigation or (if any) proceedings. May be speculatively searched against national databases.**	
Qualifying offence	**Charge**	**3 years (+ possible 2 year extension by a District Judge)**
Qualifying offence	**Arrest, no charge**	**3 years with consent of Biometrics Commissioner (+ possible 2 year extension by a District Judge)**
Minor offence	**PND**	**2 years**
Any/None (but retention sought on national security grounds)	**Biometrics taken**	**2 years with NSD by Chief Officer (+ possible 2 year renewals)**

1.3 IMPLEMENTATION OF THE NEW REGIME

LEGACY MATERIAL

14. Although PoFA gained royal assent in May 2012, its 'biometric' provisions were not brought into effect until 31 October 2013. In the meantime, a wide-ranging 'cleansing' exercise was embarked upon with a view to ensuring that material would not be being wrongfully held on the national databases when those provisions came into effect.

15. As a result, by 24 October 2013 (and according to a Written Ministerial Statement of that date[9]):

- 7,753,000 DNA samples had been destroyed;
- 1,766,000 DNA profiles had been deleted from the National DNA Database; and
- 1,672,000 fingerprint records had been deleted from IDENT1, the national police fingerprint database.

It should be noted, however, that despite those deletions some 12.5% of men and some 3% of women in the United Kingdom continued to have their DNA profiles and/or fingerprints retained on those national databases.

THE IMPORTANCE OF THE PNC

16. Whilst it is a relatively easy matter to lay down rules as to the circumstances in which DNA profiles and fingerprints can and cannot be retained by the police, it is significantly harder to devise processes which ensure that those rules are effective and that the appropriate deletions actually take place. This is particularly true in circumstances where the rules are as complicated, and the numbers are as large, as is indicated above. When the general rule is that all DNA profiles and fingerprints can be retained indefinitely, the implementation of a retention regime is simple. However, when one is dealing with hundreds of thousands of arrestees each year – and when retention or deletion of their DNA profiles and fingerprints turns on the specific history of each individual arrestee – the implementation problems are considerable.

17. In those circumstances it was quickly decided that the only sensible way of putting the new retention regime into effect was by programming the Police National Computer ('the PNC') – onto which the details of everyone who is arrested are entered – so that it would, by communicating with the National DNA Database and IDENT1, automatically drive (in appropriate cases) the deletion of arrestees' biometric records. As is explained later in this report, that process has been neither straightforward nor problem-free.

[9] See https://www.gov.uk/government/speeches/protection-of-freedoms-act-implementation-and-national-dna-database-annual-report-2012-to-2013

1.4 THE COMMISSIONER'S RESPONSIBILITIES AND OFFICE

18. As Biometrics Commissioner, I have three main responsibilities.

    i. The first is to decide applications made by the police under new section 63G of PACE – that is, applications for consent to the extended retention of DNA profiles and/or fingerprints belonging to individuals who have no convictions but who have been arrested for, though not charged with, a 'qualifying' offence.[10]

    ii. The second is to keep under review National Security Determinations which are made or renewed by Chief Officers and pursuant to which DNA profiles and/or fingerprints may be retained for national security purposes.[11]

    iii. The third is the general 'independent oversight' function that is referred to above i.e. that of *"keeping under review the retention and use"* by the police of DNA samples, DNA profiles and fingerprints.[12]

    In this report I deal with my discharge of those responsibilities in broadly that order. Save only as regards issues relating to national security, they are concerned solely with the retention and use of biometric material by police forces in England and Wales.

19. In discharging those responsibilities I have the assistance of a small staff and together we form the Office of the Biometrics Commissioner ('the OBC'). Although each member of staff is a Home Office employee, they work under my direction and solely for the OBC. They are acutely conscious of the need to operate entirely independently of outside pressure and I am satisfied that they do so. I am very grateful to them for their assistance.

[10] See (new) sections 63F(5)(c) and 63G of PACE and section 20(9) of PoFA.

[11] See section 20(2)(a) of PoFA.

[12] See sections 20(2)(b), 20(6) and 20(7) of PoFA. This general oversight function also covers the retention and use of any copies of DNA profiles and fingerprints.

2. APPLICATIONS UNDER SECTION 63G OF PACE[13]

2.1 BACKGROUND AND POLICY

GENERALLY

20. Where a person without previous convictions is arrested for, but not charged with, an offence, their fingerprints and DNA profile (their 'section 63D material') may usually be retained only until the conclusion of the investigation of that offence. If, however, that offence is a 'qualifying' offence,[14] the responsible chief officer of police may apply to the Biometrics Commissioner under section 63G of PACE for consent to the extended retention of that person's DNA profile and/or fingerprints. If the Commissioner accedes to that application, the profile and fingerprints can be retained for three years from the date that the relevant sample or fingerprints were taken.[15]

THE RELEVANT STATUTORY PROVISIONS

21. Section 63G of PACE provides as follows.

> *"(2) The responsible chief officer of police may make an application under this subsection if ... [he/she] ... considers that…any alleged victim of the offence was at the time of the offence –*
>
> *(a) under the age of 18*
>
> *(b) a vulnerable adult, or*
>
> *(c) associated with the person to whom the material relates.*
>
> *(3) The responsible chief officer of police may make an application under this subsection if ... [he/she] ... considers that –*
>
> *(a) the material is not material to which subsection (2) relates, but*
>
> *(b) the retention of the material is necessary to assist in the prevention or detection of crime.*
>
> *(4) The Commissioner may, on an application under this section, consent to the retention of material to which the application relates if the Commissioner considers that it is appropriate to retain the material.*
>
> *(5) But where notice is given under subsection (6) in relation to the application, the Commissioner must, before deciding whether or not to give consent, consider any representations by the person to whom the material relates which are made within the period of 28 days beginning with the day on which the notice is given.*

[13] Note – this section only applies to England and Wales. Different rules apply in Northern Ireland and Scotland.

[14] As has been explained earlier, a 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary: see section 65A(2) of PACE.

[15] If the date of the arrest for the qualifying offence was later than the date(s) on which the relevant sample or fingerprints were taken, the three year period will run from the date of that arrest: see section 145 of the Anti-social Behaviour, Crime and Policing Act 2014.

(6) The responsible chief officer of police must give to the person to whom the material relates notice of –

(a) an application under this section, and

(b) the right to make representations."

22. The following (among other) points will be noted as regards those provisions.

i. An application for extended retention may be made under either section 63G(2) or section 63G(3).

ii. On the face of things, a chief officer may make an application under section 63G(2) provided only that they consider that an alleged victim of the alleged offence was, at the time of that offence, under 18, "*vulnerable*" or "*associated with*" the arrestee.[16] Whereas a chief officer may only make an application under section 63G(3) if they consider that the retention of the material "*is necessary to assist in the prevention or detection of crime*", section 63G(2) imposes no express requirement that there be some anticipated public interest in the retention of the material.

iii. A chief officer may only make an application under section 63G(3) (i.e. on the basis that they consider that retention "*is necessary to assist in the prevention or detection of crime*") if they also consider that the alleged victim did not have any of the characteristics set out in section 63G(2).

iv. By section 63G(4), the Commissioner may accede to an application under section 63G(2) or (3) "*if the Commissioner considers that it is appropriate to retain the material*". No guidance is provided as to the factors which the Commissioner should take into account when deciding whether or not retention is 'appropriate'.

v. Although it is provided at sections 63G(5) and (6) that the person to whom the material relates must be informed of any application for extended retention and given the opportunity to make representations against it[17], no indication is given as to the extent (if any) to which that person must be told of the reasons for the application or of the information upon which it is based.

CONSULTATION

23. Against that background and in preparation for the commencement of PoFA, I issued a Consultation Paper in May 2013. In that paper (a copy of which can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206009/biometrics-commissioner-consultation-document.pdf) I sought comments on a variety of proposals which I had developed as to how I might proceed as regards applications for extended retention and as to the factors which I should take into account. I published that

[16] These terms are defined at section 63G(10).

[17] Further relevant provision are at sections 63G(7) to (9).

document on my webpage and sent copies to the people and organisations listed in it.[18] Having considered the responses to that Consultation Paper (almost all of which were broadly supportive of the proposals I had advanced)[19] I then published my conclusions and a number of guidance and other documents for police and public use.

CORE PRINCIPLES AND RELEVANT FACTORS

24. The approach which I decided to adopt to applications under section 63G(2) and (3) is set out in a document issued by my Office entitled *Principles for Assessing Applications for Biometric Retention.* The full document can be found at https://www.gov.uk/government/publications/principles-for-assessing-applications-for-biometric-retention and its key provisions are as follows.

> *"Core Principles*
>
> *1. The Commissioner will grant an application under section 63G(2) or (3) only if he is persuaded that the applying officer has reasonable grounds for believing that the criteria set out in those subsections are satisfied. Equally, however, he will not grant such an application merely because he is so persuaded. He will treat compliance with those criteria as a necessary, but not as a sufficient, condition for any conclusion that it is "appropriate" to retain the material at issue.*
>
> *2. The Commissioner will grant such an application – and will consider the extended retention of such material 'appropriate' – only if he is persuaded that in the circumstances of the particular case which gives rise to that application:*
>
> - *there are compelling reasons to believe that the retention of the material at issue may assist in the prevention or detection of crime and would be proportionate; and*
> - *the reasons for so believing are more compelling than those which could be put forward in respect of most individuals without previous convictions who are arrested for, but not charged with, a 'qualifying' offence.*
>
> *3. This will be the case for applications under both section 63G(2) and section 63G(3). The Commissioner will, however, be particularly alert to the possibility that extended retention may be appropriate in cases in which the criteria set out in Section 63G(2) are satisfied.*
>
> *4. The Commissioner will require that the arrestee be informed – at least in general terms – of the reasons for any application and of the information upon which it is based. If the arrestee is not so informed of any reasons or information which the applying officer seeks to rely upon, the Commissioner will attach no weight to them.*

[18] The list is on page 15 of the document.

[19] A summary of the responses can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261625/PACE_responses.pdf

Relevant Factors

5. The factors which the Commissioner will take into account when considering whether or not it is appropriate to retain material will include the following:

(i) the nature, circumstances and seriousness of the alleged offence in connection with which the individual in question was arrested;

(ii) the grounds for suspicion in respect of the arrestee (including any previous complaints and/or arrests);

(iii) the reasons why the arrestee has not been charged;

(iv) the strength of any reasons for believing that retention may assist in the prevention or detection of crime;

(v) the nature and seriousness of the crime or crimes which that retention may assist in preventing or detecting;

(vi) the age and other characteristics of the arrestee; and

(vii) any representations by the arrestee as regards those or any other matters."

OBC DOCUMENTS

25. In addition to that *'Principles'* document, my Office and I developed – and published on my webpage – a number of other documents for use by the police and by the public in connection with applications under section 63G.

DOCUMENTS FOR POLICE USE

26. These documents include:

- BC1 Application Form. This is the pro-forma application form which chief officers should use to make applications under s.63G.
- BC2 Application to the Biometrics Commissioner – Explanatory Notes. This is an explanatory document which provides guidance to chief officers on the procedure for making applications, on how to complete BC1 Application Forms and on the sorts of supporting documents (such as PNC Printouts, Crime Reports and MG3s[20]) that should accompany them.
- Notification Letter. This is a standard form letter which chief officers should use when informing the subject of an application. It also identifies the other documents which should be provided to the subject.

DOCUMENTS FOR USE BY THE PUBLIC

27. These documents include:

- BC3 Representations Form. This form is for use by individuals who wish to make representations to the Biometrics Commissioner in response to applications for

[20] An MG3 is a 'Report to Crown Prosecutor for Charging Decision'.

extended retention of biometric material. A copy of it should be enclosed with the Notification Letter.

- Applications for Biometric Retention: What You Should Know. This document explains how and when applications for extended retention can be made to the Commissioner, what the process means for individuals who are the subject of such an application, and how they can make representations. A copy of it should also be enclosed with the Notification Letter.

STRATEGY BOARD GUIDANCE

28. The Protection of Freedoms Act specifies that the National DNA Database Strategy Board may issue guidance about the circumstances in which applications may be made to the Biometrics Commissioner under section 63G, and that before issuing any such guidance that Board must consult the Commissioner.[21] The Strategy Board endorsed the approach which I had decided to adopt as regards such applications and the detailed Guidance document which it issued in September 2013 (and into which I had significant input) is consistent with the *'Principles'* and other documents that have been issued by my Office. A copy of the Strategy Board Guidance can be found at https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace.

THE TIMING OF APPLICATIONS AND 'THE CONCLUSION OF THE INVESTIGATION OF THE OFFENCE'

29. By section 63E of PoFA, the police are entitled to retain an arrestee's DNA profile and fingerprints until "*the conclusion of the investigation of the offence*" in which that person was suspected of being involved ("*or, where the investigation gives rise to proceedings against the person for the offence, until the conclusion of those proceedings*"). It follows from that, of course, that there can be no need for an application for extended retention before that stage is reached i.e. (in the case of someone who has been arrested but not charged) until after *"the conclusion the investigation of the offence"*. The Act contains no definition of that term.

30. The issue of what should count as *"the conclusion of the investigation of the offence"* was debated in the House of Lords on 29 November 2011[22]. An amendment was moved (and then withdrawn) by Baroness Hamwee as follows:

> *"5: Clause 2, page 2, line 41, at end insert-*
>
> *'( ) For the purpose of this section, an investigation is concluded when it is so certified by the responsible chief of police.'"*

[21] See section 24 of PoFA which introduced (new) section 63AB(4) and (5) of PACE.

[22] See Hansard http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111129-0001.htm#11112947000486

31. It was noted by Lord Dear that:

> *"There are thousands of offences on police books and well over half of them remain undetected. Therefore, seeking a certificate for every single one of them when one believed that an investigation was concluded would frankly be a bureaucratic nightmare. Quite apart from that, at the very serious end of offences it is not uncommon to have 50, 80 or 100 detectives and others working on an investigation. As the case winds on, that number will be run down until, months or even years later, you finish with perhaps five or six. There will come a point when everyone will know that the investigation has stopped because they will simply have run out of avenues to explore, but in my experience no chief officer would wish to say categorically, "It is finished", because that would be slamming a door in the face of victims. We have already spoken in your Lordships' House about the need to balance the rights and feelings of victims among other things, and that is absolutely right. I do not think that any chief officer of police would wish to say, "We have now certified that this is finished and as far as you, the victim, are concerned – or you, the general public, are concerned – we have now closed our books", and I do not believe that the public would wish to hear it."*

32. Whatever the force of the points made by Lord Dear, real difficulties arise as a result of the fact that the retention period for an individual's biometric material is, by PoFA, tied to the concept of *"the conclusion of the investigation of the offence"*. Quite apart from the scope for argument as to precisely when that stage has been reached in the particular circumstances of any given case, two particular difficulties arise.

    i. There is an important distinction between the investigation of an offence and the investigation of an individual's suspected involvement in that offence – and it is clear that the former may last a great deal longer than the latter. Given the thinking which appears to have lain behind the introduction of the retention regime established by PoFA, it would seem surprising if, even in circumstances where an individual of good character has been quickly and conclusively eliminated as a suspect for the offence for which they were arrested, their biometric records could nonetheless be retained on the national databases for as long as the investigation into that offence continues. As Lord Dear pointed out, *"at the very serious end of offences"* it is not uncommon for an investigation to last for months or even years.[23]

    ii. As is pointed out above, it was quickly decided that the only sensible way of putting the new retention regime into effect was by programming the PNC so that it would, by communicating with the National DNA Database and IDENT1, automatically drive

[23] See also the remarks of James Brokenshire MP on 29 March 2011:

"Turning to the broader point at issue in clause 2, it might assist the Committee if I explain in a little more detail what we mean by the "conclusion of the investigation" or the "conclusion of those proceedings". ... If a person is arrested for an offence but is not charged with it, for the purposes of this clause the investigation is concluded when the person from whom the material was taken is no longer suspected of having committed that offence. That might be, for example, when another person has been arrested, or once an alibi has been checked out."

http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/110329/am/110329s01.htm (at column 197)

(in appropriate cases) the deletion of arrestees' biometric records. For the PNC to drive the deletion of the biometric records of an arrestee who has no previous convictions and is never actually charged with an offence, there has to be an entry on the PNC that will tell it that the time has come to delete them. The PNC deals with individuals and not with offences and there is no provision for the making of an entry on PNC to the effect that the investigation of an offence has reached a conclusion. There is, however, provision for the making of an entry on PNC to the effect that No Further Action ('NFA') is to be taken against an arrestee – and the 'NFA-ing' of an arrestee is generally seen as, in effect, indicating that any active investigation of that arrestee's suspected involvement in the offence for which he or she was arrested has come to an end.

33. In those circumstances it was decided – I think sensibly – that the best (and only practical) course was:

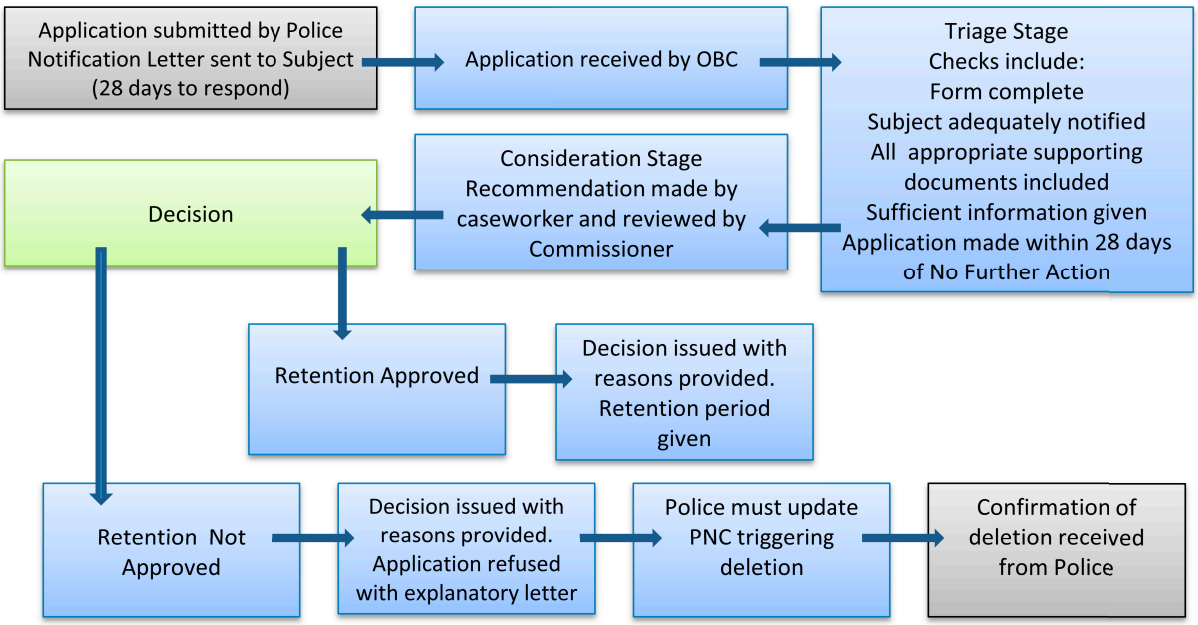
- to treat the moment at which an arrestee is NFA'd as being the moment at which the investigation of the relevant offence should usually be deemed to have reached a 'conclusion'; and
- to treat the making of an NFA entry on the PNC as (in appropriate cases) the trigger for the automatic deletion of the arrestee's biometric records from the National DNA Database and IDENT1.

34. I decided to adopt a similar approach as regards applications under section 63G and to require that such an application must usually be made within 28 days of the date on which the relevant individual is NFA'd. [In any event, unless an appropriate 'marker' is placed on the PNC within 14 days of the making of an NFA entry (i.e. a 'marker' which indicates that an application under section 63G has been or may be made), the biometric records of an individual without previous convictions who has been arrested for, but not charged with, a qualifying offence will automatically be deleted.]

PROCEDURE AND PROCESS

35. I was concerned that the process for making and deciding applications under section 63G should be as straightforward as possible and that unnecessary work and bureaucracy should be avoided. There is, however, an inevitable tension between the obvious desirability of minimising the demands which that process makes on police resources and the need to act fairly towards the individuals in respect of whom those applications are made. Even in the absence of representations from those individuals there could be no point in providing for an independent Commissioner to decide such applications if he or she is to engage in nothing more than a 'tick-box' exercise and/or is to accept without evidence or question whatever is said by the applying officer.

36. The steps which are required of the applying officer are set out in the various documents which are referred to above. The casework process which is adopted within the OBC is as indicated below.



37. It will be noted that, as fairness clearly requires, reasons are given for every decision that I make on an application under section 63G. It should also be noted that any such decision may be subject to Judicial Review on the application of either the individual affected or the applying officer.

PILOT EXERCISE

38. In preparation for the commencement of PoFA, I conducted a casework pilot for Section 63G applications between 2 and 11 October 2013. I invited 10 forces to identify 2 or 3 (legacy) cases each that appeared to them to meet the requirements for applying for extended retention of biometric material and to submit in respect of each of those cases:

- a completed BC1 PACE Application Form together with appropriate supporting documents; and
- a draft Notification Letter to the subject informing them of the application, of its substance, and of their right to make representations in response.

Forces were in effect being asked to submit 'dummy' applications based on the facts of real cases, including what might be termed 'borderline' cases.

39. During the pilot 13 'dummy' applications were received in total. The cases typically involved arrests for rape or sexual offences involving children. All the applications were evaluated by my Office and 'indicative decisions' and feedback were provided. Following the conclusion of the pilot exercise, a 'Lessons Learnt' document was issued to all forces.

40. An important issue was identified during the pilot exercise which, if it had not been addressed before PoFA came into effect, might well have meant that that it would thereafter have been unlawful for police forces to retain large numbers of DNA profiles and fingerprints which it had clearly been expected and intended that they should be able to retain. This problem arose out of the fact that, whereas it had long been common for police to take a DNA sample only after a first arrest, the retention regime which was provided for by PoFA assumed that a fresh DNA sample and fresh fingerprints would be taken on every arrest.[24]

41. I alerted the Home Office to this problem and an interim solution was effected immediately before commencement by the making of the *Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) (No.2) Order 2013.* The problem was ultimately resolved by section 145 of the Anti-social Behaviour, Crime and Policing Act 2014.

OTHER ENGAGEMENT WITH POLICE FORCES

42. Before conducting the pilot exercise I had asked every force to nominate a single point of contact (a 'SPOC') who would be responsible for co-ordinating applications to me under section 63G. On numerous occasions before and after the relevant provisions of PoFA came into effect, I have written (or my Office has written on my behalf) to those SPOCs and/or to chief officers about the scope for such applications and about various aspects of the application process. In June of 2014 I gave a presentation about that process at an ACPO Professional Development Event in Warwickshire and, some days later, my Office held a Conference/Seminar for SPOCs and others in Birmingham to discuss that process, to promote best practice, and to identify and address any concerns which forces might have about it.

2.2 APPLICATIONS RECEIVED

VOLUMES

ESTIMATES

43. One of the central difficulties I faced when trying to establish a system to deal with applications for extended retention was that of predicting the number of such applications that were likely to be made. At an early stage it was suggested to me that that number could be tens of thousands each year.

[24] In circumstances where all arrestees' DNA samples were subject to indefinite retention there was, of course, little point in taking more than one sample from the same individual.

44. After I had published my '*Principles*' document – and had thus made clear the approach which I intended to adopt to applications under section 63G – I requested formal estimates from police forces. The responses which I received in September of 2013 indicated that I could expect around 60 applications per month. In April of 2014 – and after the relevant provisions had been in force for some six months – revised estimates were submitted which indicated that a more likely figure would be around 30 applications per week.

ACTUAL

45. In the event, however, the number of applications which I have actually received has been substantially lower than was estimated. In particular, in the 10 months after the relevant sections of PoFA came into force on 31 October 2013 (i.e. in the period to 31 August 2014) only 91 applications were received.

46. There are a number of possible explanations for that relatively small number and I return to them later in this report. At this stage, however, two factors merit particular mention.

    i. As brought into effect, PoFA only allows for applications under section 63G in circumstances where the individual in question has been arrested after 31 October 2013.[25] Since no application would be necessary unless and until that individual had then been investigated and NFA'd, it was always unlikely that many applications would be made in the first 2 or 3 months of the new regime. In the event only 3 applications were made before 1 February 2014 and one of those was ineligible because the relevant arrest was in July 2013.

    ii. All but 3 of the 91 applications that were made by 31 August 2014 were made by the Metropolitan Police Service (the 'MPS'). Since the MPS accounts for about 20% of arrests in England and Wales, it seems likely that if all other forces had engaged with the application process in a similar way, the total number of applications by 31 August 2014 would have been around 450 – 500. If, moreover, the MPS and other forces were to make applications at a similar rate to that at which they were made by the MPS in July and August of 2014, the total number of applications per annum would be of the order of 1,200.

[25] http://www.legislation.gov.uk/uksi/2013/1813/article/4/made

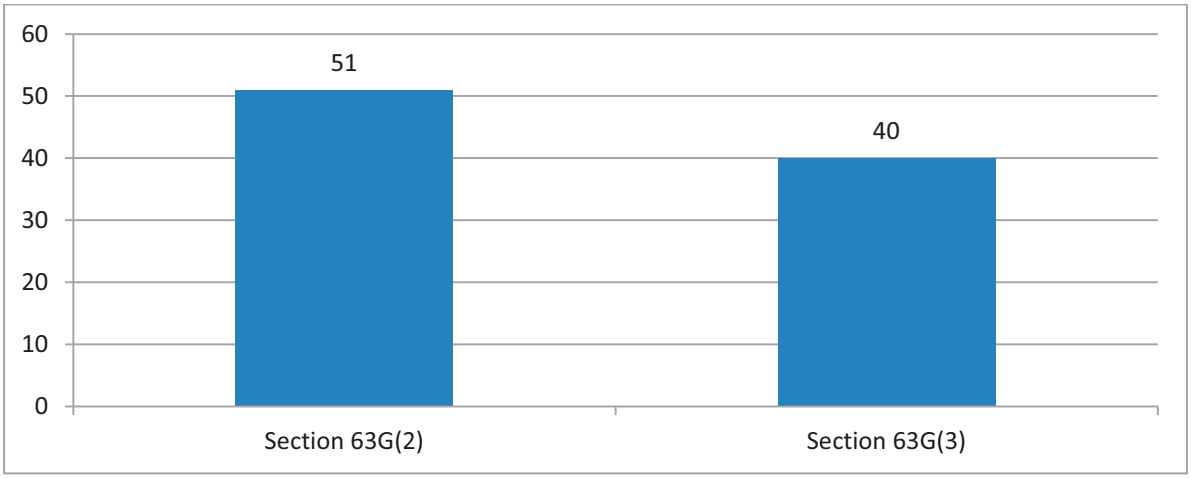
APPLICATIONS: STATISTICAL ANALYSIS

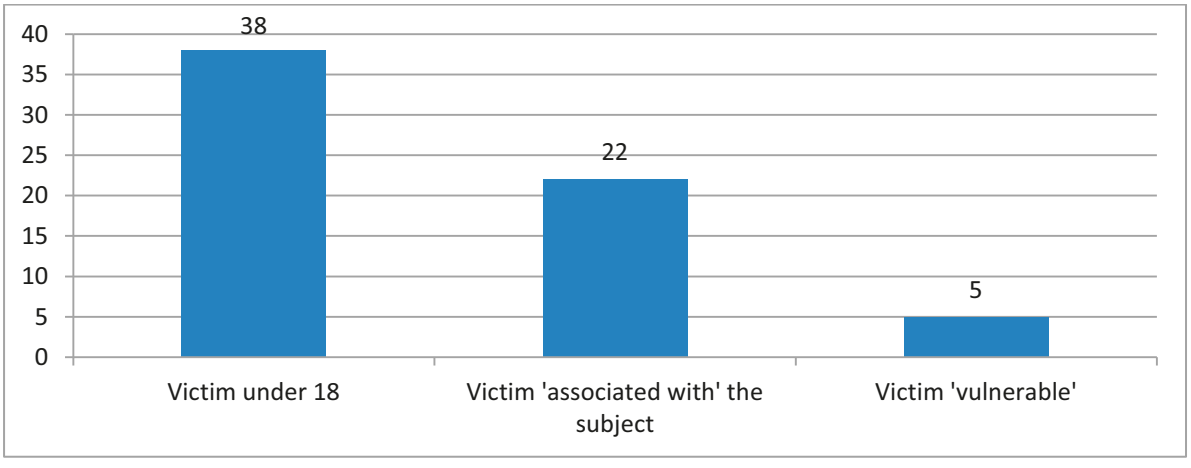
47. The following are features of the 91 applications made between 31 October 2013 and 31 August 2014.

STATUTORY BASIS FOR APPLICATIONS

48. 51 applications were made under section 63G(2) and 40 were made under section 63G(3).[26] In a number of the former applications more than one of the 'victim criteria' were satisfied; overall, however:

- in 38 of the applications under section 63G(2) the alleged victim was under 18 years of age;
- in 22 the alleged victim was 'associated with' the subject of the application; and
- in 5 the alleged victim was 'vulnerable'.

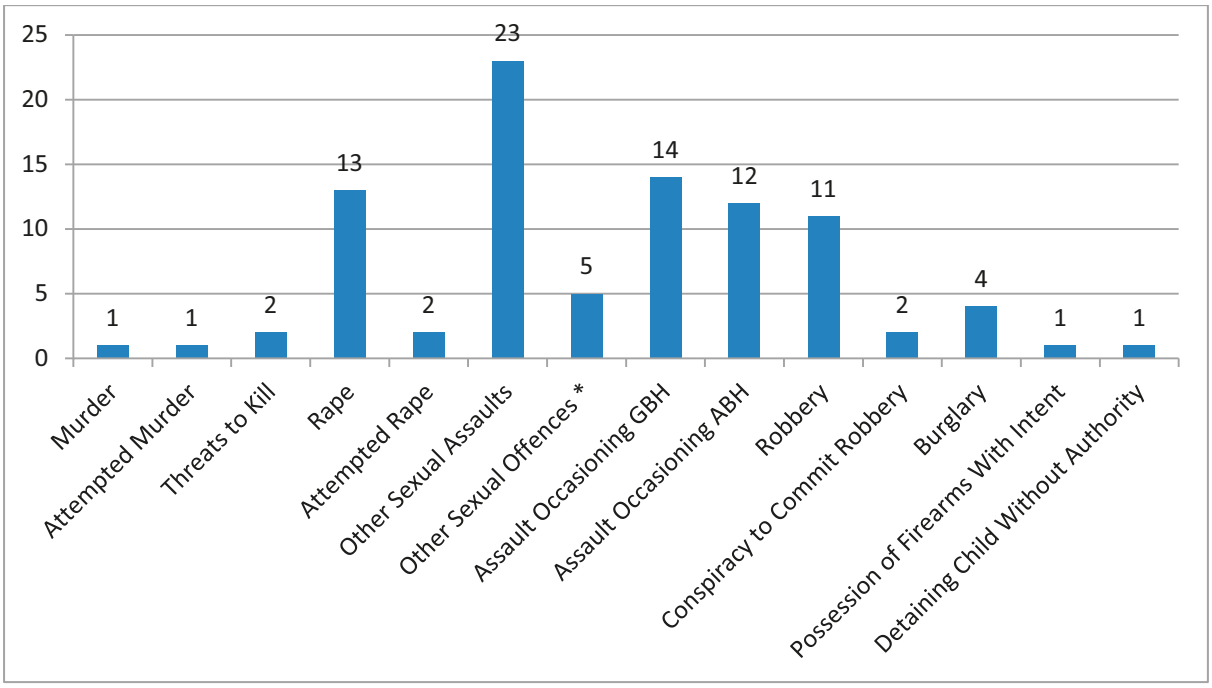




[26] In a few application forms the wrong provision was referred to and/or it was unclear which provision was being relied on. In all cases where the section 63G(2) 'victim criteria' were apparently satisfied, my Office has treated the application as being made under that provision.

QUALIFYING OFFENCES

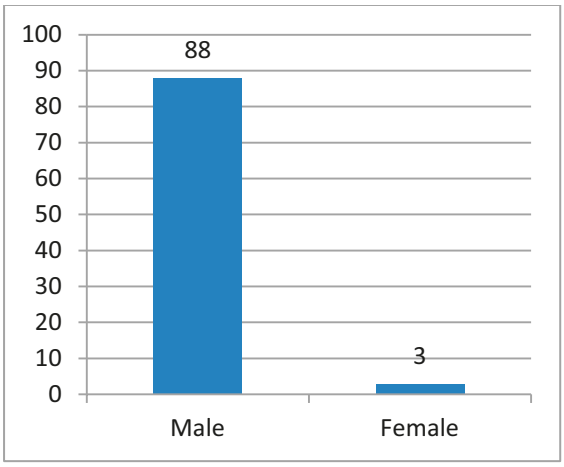
49. The qualifying offences for which the subjects of those 91 applications were arrested were as follows[27].



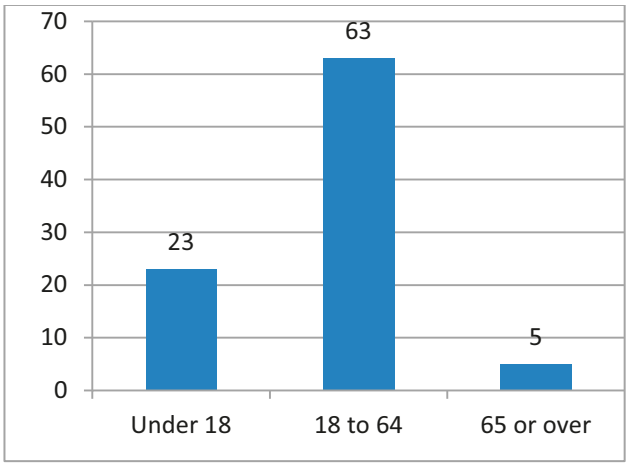
* The 'Other Sexual Offences' were 3 x Indecent Exposure, 1 x Voyeurism and 1 x Causing a child to watch/look at an image of sexual activity.

SUBJECT CHARACTERISTICS

SEX

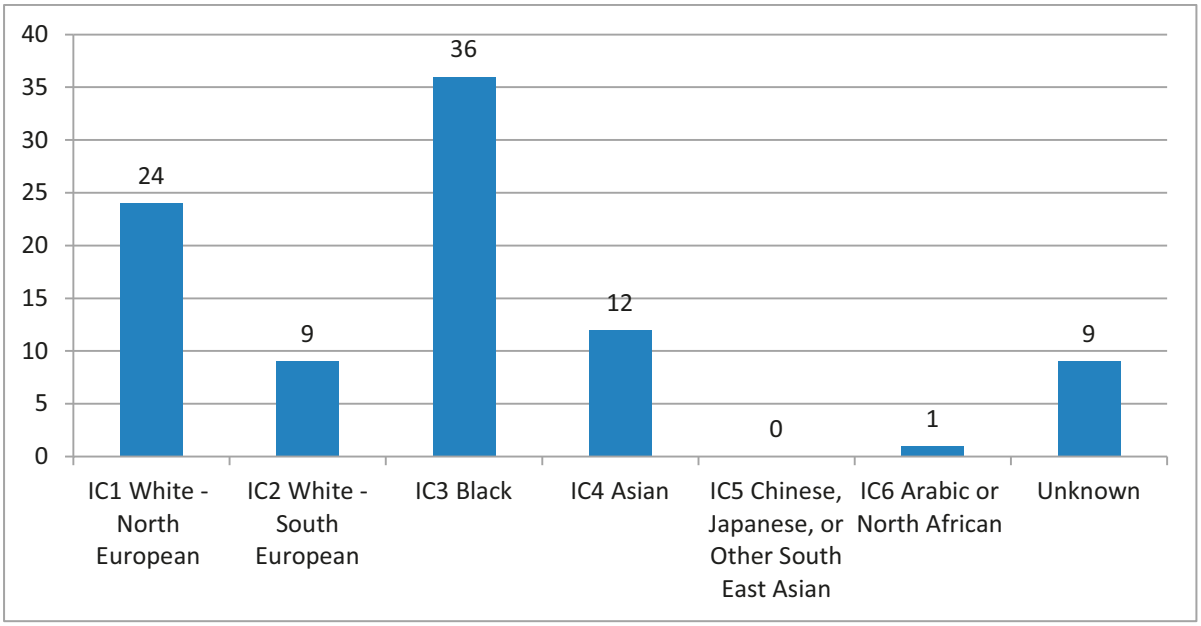


AGE



[27] Note: for two subjects, applications were made in respect of more than one qualifying offence.

ETHNICITY[28]



PREVIOUS ARRESTS ETC.

50. Of the 91 subjects, 77 had been previously been arrested and/or had previously had allegations or complaints made against them. Of those 76, 64 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.

OUTCOME OF APPLICATIONS: STATISTICAL ANALYSIS

51. Of the 91 applications made by 31 August 2014, 40 had been concluded by that date.[29] Of those 40, 25 had been approved, 5 had been refused, and 10 had been withdrawn.

STATUTORY BASIS FOR APPLICATIONS

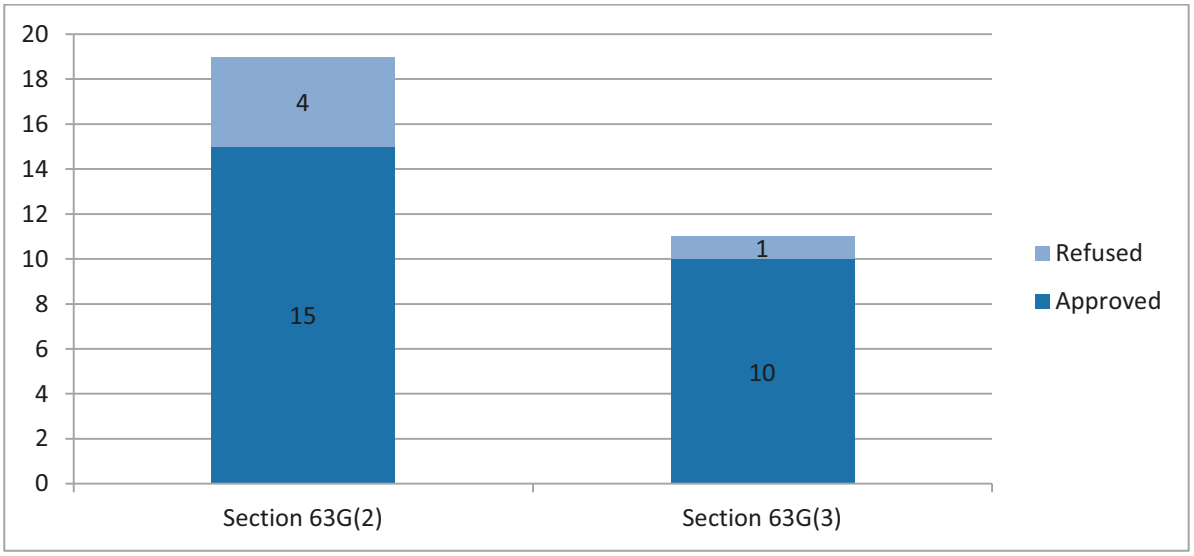
52. Of the 25 applications which had been approved by 31 August 2014, 15 were made under section 63G(2) and 10 under section 63G(3). In a number of the former applications more than one of the 'victim criteria' were satisfied; overall, however:

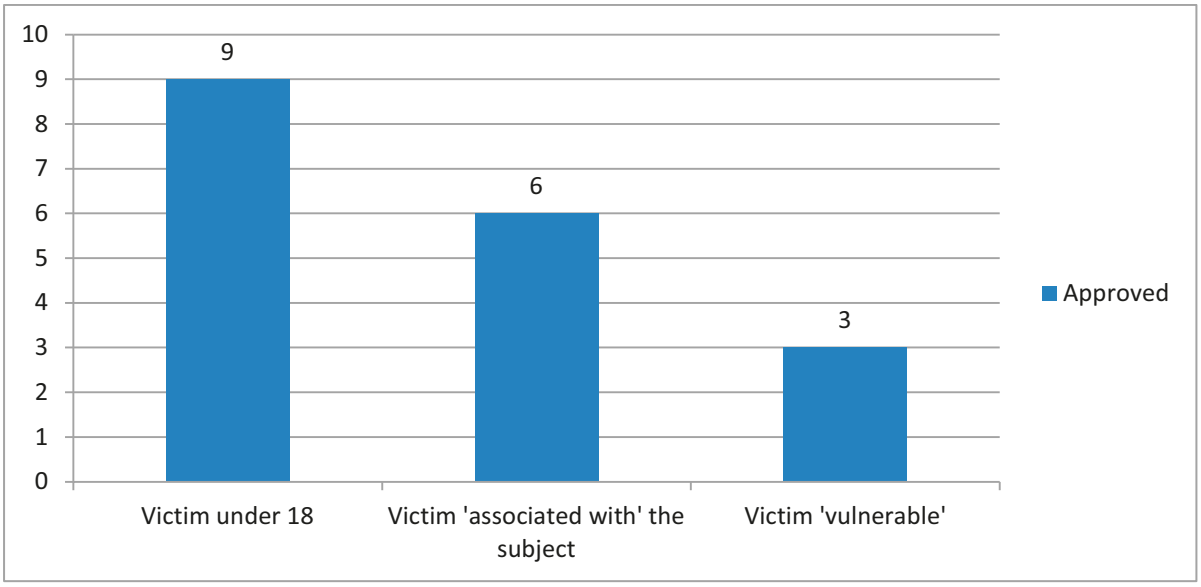
- in 9 of the applications under section 63G(2) the alleged victim was under 18 years of age;
- in 6 the alleged victim was 'associated with' the subject of the application; and
- in 3 the alleged victim was 'vulnerable'.

[28] 'Ethnicity' here refers to a police officer's visual assessment of a person's ethnic appearance rather than a subject's self-defined ethnicity. See http://policeauthority.org/metropolitan/publications/briefings/2007/0703/index.html for the code systems used by the Metropolitan Police Service (MPS) to record ethnicity.

[29] There is, of course, an inevitable delay between the making of an application and its determination, not least in view of the need to allow time for representations to be made by the subject of the application and for those representations to be considered by the Commissioner.

53. 1 of the 5 applications which had been refused by 31 August 2014 was refused as ineligible because the relevant arrest had been made before 31 October 2013. Of those 5 applications, 4 were made under section 63G(2) and 1 under section 63G(3).





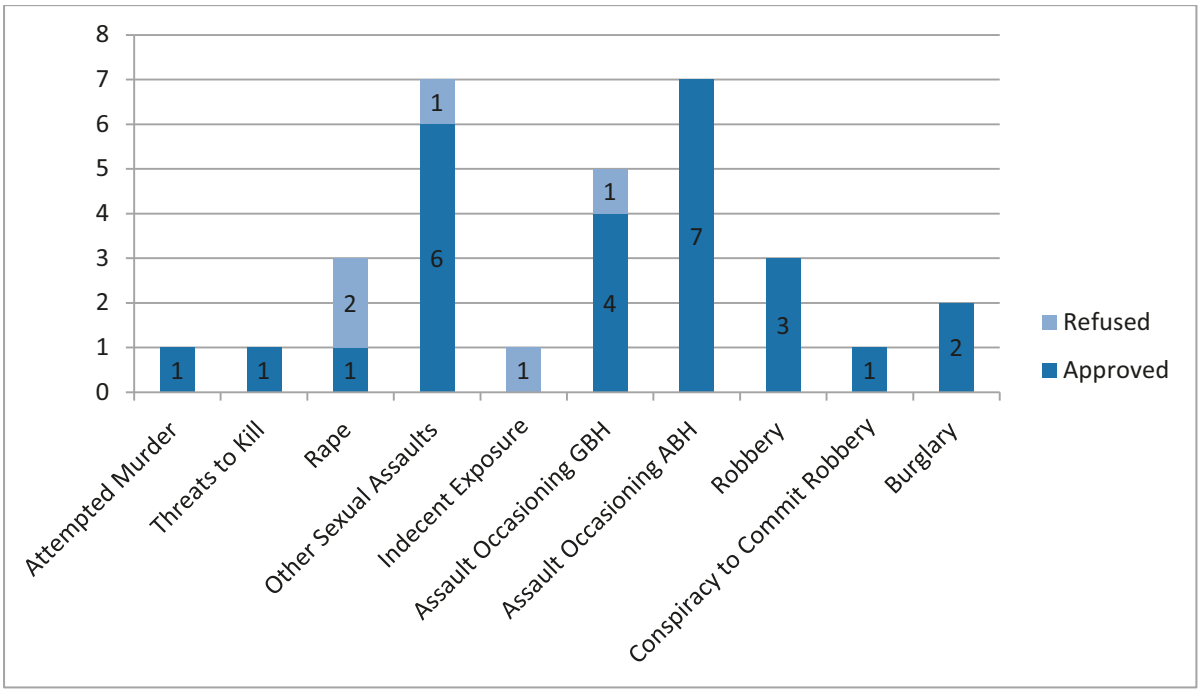
REPRESENTATIONS

54. In 6 of those 25 applications approved, representations were made by or on behalf of the individual affected.

In 2 of the 5 applications refused, representations were made by or on behalf of the individual affected.

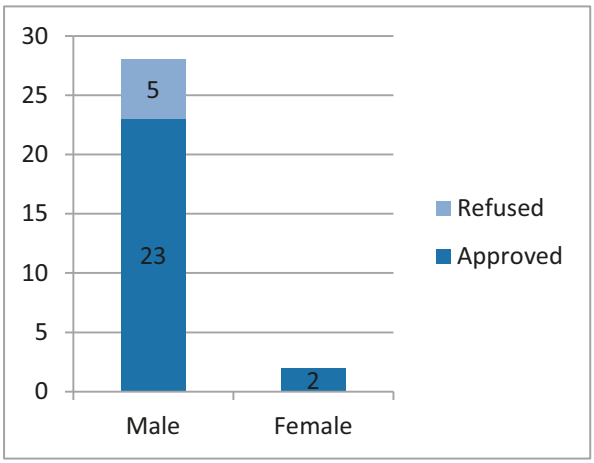
QUALIFYING OFFENCES

55. The qualifying offences for which the subjects of those 30 applications were arrested were as follows[30].

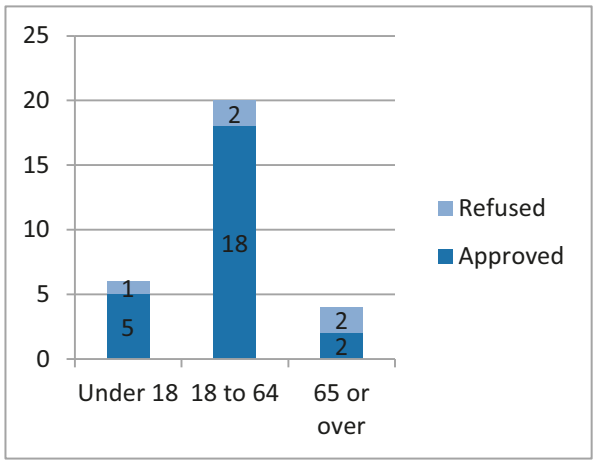


SUBJECT CHARACTERISTICS

SEX

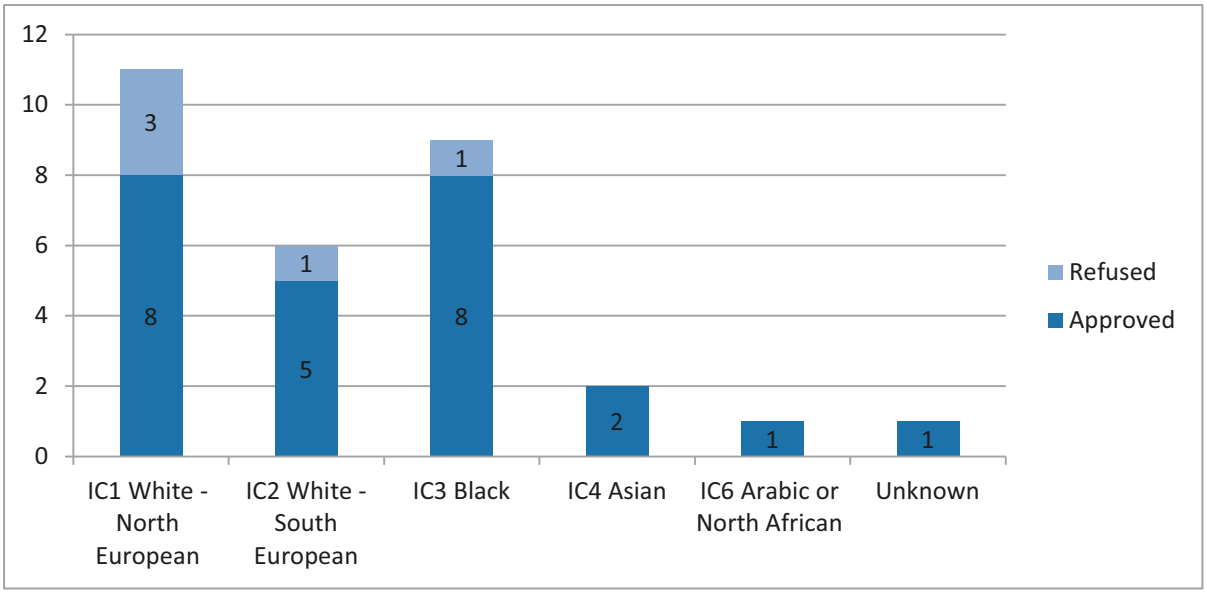


AGE



[30] Note: one of these applications was made in respect of two qualifying offences.

ETHNICITY



PREVIOUS ARRESTS ETC.

56. Of the subjects of the 25 applications which had been approved, 21 had been previously been arrested and/or had previously had allegations or complaints made against them. Of those 21, 20 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.

57. Of the subjects of the 5 applications which had been refused, 4 had been previously been arrested and/or had previously had allegations or complaints made against them. Of those 4, 3 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.

APPLICATIONS WITHDRAWN

58. Of the 10 applications which had been withdrawn by 31 August 2014:

- 1 was withdrawn when it was pointed out that it was ineligible as the relevant arrest had been made before 31 October 2013;
- 3 were withdrawn because the subject had been convicted of a recordable offence after the application was submitted (and because their biometric records could therefore be retained indefinitely);
- 1 was withdrawn when it was discovered that the relevant biometric records had been already been deleted because of the force's failure to put an appropriate 'marker' on PNC;[31] and

[31] The application was made in respect of an allegation of sexual assault against a female.

- 5 were withdrawn when it was discovered that the relevant biometric records had been already been deleted by reason of a PNC programming error.[32]

I return to those last 2 points later in this report.

PRELIMINARY APPLICATIONS, INTERIM NOTIFICATIONS AND ONGOING COMPLEX INVESTIGATIONS

PRELIMINARY APPLICATIONS

59. I anticipated that forces might well have concerns about the extent to which, in the context of applications under section 63G, they would be required to disclose confidential information (e.g. intelligence material) to arrestees. My Office and I therefore set up, and notified forces of, a procedure for so-called 'Preliminary Applications'. By that procedure it is open to a chief officer to raise any such disclosure concerns with me before they launch a formal application or send a Notification Letter.

60. Contrary to my expectations, concerns about disclosure have yet to arise. In the period to 31 August 2014, no Preliminary Applications were made and in none of the 91 applications that were made was disclosure raised as a problem.

INTERIM NOTIFICATIONS

61. In the early months of 2014 a significant number of cases about which my Office was approached involved subjects who had not been charged with the qualifying offences for which they were arrested but who had been charged with lesser 'non-qualifying' offences relating to the same incidents (e.g. they had been arrested for Assault Occasioning Actual Bodily Harm but had been charged only with Battery).

62. The question arose as to how best to deal with the practical difficulties associated with such cases i.e. cases where:

- in the absence of an application under section 63G, the subject's biometric records would be deleted if they were acquitted of the 'non-qualifying' offence with which they had been charged; but
- the need for such an application would be negated if the subject in fact chose to plead guilty to that lesser offence and/or was found guilty of it at trial.

Those difficulties were compounded by the fact that, in line with the guidance issued by my Office and by the Strategy Board, an application under section 63G must usually be made within 28 days of the subject being NFA'd for the relevant qualifying offence.

63. I had initially taken the view that, in order to ensure fairness to subjects, that 28 day time-limit should normally apply even in cases of this sort. On further consideration, however,

[32] These applications were made in respect of allegations of rape, inciting a child to perform a sexual act, indecent exposure, voyeurism and ABH.

and when it became apparent that such cases might well be much more common than I had at first envisaged, I concluded that a different approach would be preferable. In April of 2014 I therefore wrote to all forces to provide them with revised guidance in this connection.

64. My revised guidance was that in such circumstances – and rather than making an application under section 63G as soon as it was decided that the qualifying offence should be NFA'd – the relevant Chief Officer should write to the subject informing him or her that such an application might be made in due course. This is known as an 'Interim Notification' and it does not require any action by the subject at that point. I made clear that, provided that the subject has been notified of a potential application within 28 days of the decision to charge him or her with a lesser offence (and thus to NFA the qualifying offence), I will generally be content to accept a later section 63G application 'out of time'.

65. If an Interim Notification letter is sent out:

- the subject receives fair and prompt notice of the fact that an application for extended retention may later be made even if they are acquitted of the lesser offence with which they have been charged; but
- extensive work and resources need not be devoted to the making of a section 63G application which may later prove to have been unnecessary.

This seems to me a fair and sensible arrangement for all concerned.

66. Forces have been asked to inform me of any Interim Notifications which they give and to provide my Office with regular updates on the progress of the relevant prosecutions. In the period between 31 October 2013 and 31 August 2014 my Office was informed of 32 Interim Notifications, all of them by the MPS. As at that latter date, 2 of those Notifications had been followed by applications under section 63G and 7 had 'lapsed' as the individuals in question had been convicted of recordable offences (and their biometric records had therefore become subject to indefinite retention).

ONGOING COMPLEX INVESTIGATIONS

67. I recognise:

- that there will sometimes be cases in which an arrestee will be NFA'd even though the relevant investigation remains ongoing and they remain a suspect for the offence for which they were arrested; and
- that in such circumstances the continued retention of their biometric material may be justifiable according to both the letter and the spirit of the new PoFA regime.

One such case was brought to my attention in December of 2013.

68. After receiving a full briefing on all the facts of the case, I was satisfied:

- that the investigation at issue was continuing both as regards the offence itself and the suspected involvement of named individuals in it;
- that those named individuals remained suspects for the offence even though it had been decided that there was insufficient evidence to charge them and that they should be NFA'd rather than kept on police bail;
- that in those circumstances their DNA profiles and fingerprints could lawfully be retained; and
- that those profiles and prints might well prove to be of value to the continuing investigation.

I was also satisfied, however, that as a result of the NFA-ing of those individuals and the recording of that step on the PNC, their DNA profiles and fingerprints would automatically (and irrevocably) be deleted unless action was quickly taken to prevent that deletion.

69. In those circumstances I agreed that the police should place a 'UZ' (or 'Biometrics Commissioner') marker on the PNC in respect of each of the individuals concerned. The effect of such a marker is to prevent until further notice the automatic deletion of biometric records. I also asked for – and have obtained – quarterly updates on the case from the police so that I can satisfy myself that the relevant investigation is continuing and that the retention of those records continues to comply with both the letter and spirit of the new regime. I am satisfied that it does.

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

70. Under the PoFA regime the DNA profile and/or fingerprints of a person without previous convictions may be retained for an extended period of 3 years if:

- the Biometrics Commissioner consents to such retention following an application under section 63G of PACE; or
- that person is not merely arrested for, but also charged with, a qualifying offence.

By section 63F of PACE, moreover,[33] that 3 year period may be extended for a further 2 years if, following an application by the relevant Chief Officer under section 63F(7), a District Judge so orders.

71. As yet there has, of course, been no scope for an application under section 63F(7) in respect of an individual in relation to whom a successful application has been made under section 63G. As regards individuals who have been charged with (though not convicted of) qualifying offences, however, it has since 31 October 2013 been open to the police to make such applications provided that the relevant DNA profiles and/or fingerprints would otherwise have been subject to automatic deletion on or after 31 January 2014.

[33] (as inserted by section 3 of PoFA)

72. In the event it appears that only 6 such applications were made to District Judges between 31 October 2013 and 31 August 2014 and that all of them were made by the MPS. All of those applications were successful and in each of them the District Judge gave detailed reasons for his or her decision. My Office has sought and obtained copies of the written applications that were made and of the written rulings that were given in each of those cases.

2.3 ISSUES ARISING FROM APPLICATIONS MADE

THE VALUE/USEFULNESS OF RETENTION

73. The central issue which arises in almost every application under section 63G is that of whether *"in the circumstances of the particular case which gives rise to that application … there are compelling reasons to believe that the retention of the material at issue [i.e. the retention of the DNA profile and/or fingerprints of the subject of the application] may assist in the prevention or detection of crime …"*

74. There will rarely be compelling reasons to believe that the continued retention of a subject's DNA profile or fingerprints may assist in the investigation or prosecution of the (alleged) qualifying offence which is relied on in the application. That investigation will almost always have been concluded and that individual will invariably have been NFA'd for that offence notwithstanding the availability of their biometric records. [34] If, moreover, the investigation of that offence is 'resumed' after the deletion or destruction of the subject's DNA profile and/or those fingerprints, it will usually be open to the police to take a further DNA sample from them and/or to re-take their fingerprints.[35]

75. There will, moreover, seldom be compelling reasons to believe that the continued retention of a subject's DNA profile or fingerprints may assist in the investigation or prosecution of past offences other than the qualifying offence for which they were arrested. That profile and those fingerprints will almost always have been loaded to the relevant national databases and searched against the profiles and fingerprints on those databases from 'unsolved' crime scenes. If those searches have disclosed anything which suggests that the subject might have committed another offence, it will almost always be open to the police

[34] As is explained at paragraphs 67-69 above, if there is a continuing investigation into an arrestee's alleged involvement in an offence notwithstanding the fact that that arrestee has been NFA'd:

- the retention of their biometric material will be justifiable according to both the letter and spirit of the PoFA regime; and
- there will therefore be no need for the police to make an application to me under section 63G.

As is also explained in those paragraphs, however, it will be sensible for the police to seek my approval to the placing of a UZ maker on the PNC so as to ensure that that material is not automatically deleted before that investigation is concluded.

[35] See section 144 of the Anti-social Behaviour, Crime and Policing Act 2014.

to arrest the subject for that offence and, if they wish, to take a further DNA sample and fingerprints from them.

76. In the great majority of applications under section 63G, therefore, the police have focused on the contention that there are compelling reasons to believe:

- that the subject of the application may commit offences in the future; and
- that the retention of their DNA profile and/or fingerprints may assist in the investigation or prosecution of any such future offences.

As to the first of those matters reliance has often (and unsurprisingly) been placed on the police's previous dealings with the subject and, in particular, on previous occasions when they have had reasonable grounds to suspect that the subject has committed an offence. As to the second of those matters (and as is pointed out in my '*Principles*' document[36]) a relevant consideration will be whether the offences which it is feared that the subject may commit in the future "*are of a type in relation to which DNA or fingerprint evidence is commonly of significance*".

77. In many of the applications to me it has been contended that the relevant feared future offences are indeed of that type. In particular, it has been contended:

- that there is reason to fear that the subject will commit violent or sexual offences in the future; and
- that DNA and/or fingerprint evidence is commonly of value as regards such offences in that it may (a) lead to the identification of offenders and/or (b) corroborate the accounts given by victims or witnesses and/or (c) provide grounds for a conviction in circumstances where (e.g. for reasons of age, illness or disability) victims or witnesses decline, or are unable, to assist the prosecution.

78. Important though that these matters are, the mere fact that DNA and/or fingerprint evidence is commonly of value in the investigation or prosecution of offences of the type that it is feared that a subject may commit in the future will not, of course, always lead to the conclusion that there are compelling reasons to believe that some useful purpose may be served by the *retention* of that subject's biometric records. In particular, it may well be difficult to draw such a conclusion where, if the subject does commit such an offence, they will almost certainly be identifiable by the victim of that offence and/or will immediately be an obvious suspect for it. In such circumstances it will usually be open to the police to arrest the subject for that offence and to take DNA and fingerprints from them at that stage. It is most unlikely that reliance will have to be placed on a DNA profile or fingerprints that have been obtained from the subject on some earlier occasion.

79. This issue has arisen in a number of the applications which have been made to me under section 63G(2), particularly in the context of alleged domestic violence where the offences

[36] (at Paragraph 8)

which it is feared that the subject may commit in the future are offences of a similar nature against the same alleged victim. It is in my view an inescapable aspect of such cases that there will rarely be *"compelling reasons to believe that the retention of the material at issue may assist in the prevention or detection of crime"*.

GROUNDS FOR SUSPICION AS REGARDS THE 'QUALIFYING' OFFENCE

80. In my '*Principles*' document[37] it is pointed out that:

> *"… the less compelling the reasons for suspecting that the arrestee committed the offence in connection with which he or she was arrested, the less likely that the Commissioner will consider it appropriate to retain any biometric material which was obtained from him or her."*

That general proposition played an *important* part in my decision on one of the applications that I refused.

81. In that case it was clear that, although the subject had been arrested for a qualifying offence:

- there was no evidence whatsoever that he had committed that offence; and
- the police had concluded that *"a more appropriate charge would be one of s.4A Public Order Act 1986"* (i.e. a *non*-qualifying offence).

[This was a relatively early application and the subject had in fact been charged with that lesser offence. In similar circumstances – and since the introduction of the system of Interim Notifications[38] – a formal application would not now be made until after that lesser charge had been dealt with.]

82. In the letter which explained my reasons for refusing that application I pointed out:

- that absent an arrest for a qualifying offence – and no matter how strong may be the grounds for suspecting that an arrestee has committed an offence other than a qualifying offence – an application in respect of that arrestee cannot be made or granted under section 63G; and
- that against that background it would, in my view, rarely, if ever, be appropriate to make or grant an application under that section in circumstances where there were and are, in reality, no reasonable grounds to suspect that the subject committed the alleged qualifying offence for which he was arrested.

I remain of that view.

83. A similar issue arose in another case in which I refused an application under section 63G(2). Although in that case the subject had been arrested for GBH with Intent, the Investigating Officer had concluded that the CPS 'charging standard' for that offence had not been met

[37] See https://www.gov.uk/government/publications/principles-for-assessing-applications-for-biometric-retention

[38] See paragraphs 61-66.

and that the appropriate charge would have been one of Common Assault. Common Assault is not a qualifying offence and one (albeit only one) of the factors which led me to refuse that application was the weakness of the reasons for suspecting that a qualifying offence had in fact been committed.

MENTAL HEALTH/*MENS REA* ISSUES

84. An application for extended retention will only be granted if *"there are compelling reasons to believe that the retention of the material at issue may assist in the prevention or detection of crime… ."* In a number of applications, however, the subject has been suffering from mental health problems (such as schizophrenia or dementia) which have appeared to render them unable to exercise proper control over their actions. In those circumstances questions have arisen as to whether or not the feared future behaviour of those subjects would constitute 'crime' in the strict sense of that term. Indeed, in one such case the principal reason for not charging the subject with the qualifying offence for which they had been arrested was that they had shortly thereafter been admitted to hospital pursuant to an application under section 2 of the Mental Health Act 1983.

85. Subjects may, of course, present a significant and continuing risk to public safety whether or not they are able to exercise proper control over their actions, and it is right that reasonable steps be taken to protect the public against that risk. I have concluded that it is right for me to proceed on the basis that the retention of biometric material may *"assist in the prevention or detection of crime"* if it may assist in preventing an action, or in detecting the perpetrator of an action, which would constitute a crime if the perpetrator was of full mental capacity.

86. However, I have also concluded that, when dealing with applications for the extended retention of the biometric records of subjects who suffer from mental health problems – or, indeed, who are in any other way 'vulnerable' – it is right that, as in the case of applications in respect of juveniles, "*particular attention should be paid to …* [their] *… protection … from any detriment that may result from the retention … of their private data*."[39]

DETERRENCE

87. In a substantial proportion of applications under section 63G reliance has been placed on the proposition that the extended retention of a subject's DNA profile or fingerprints may *"assist in the prevention ... of crime"* in that it may deter that individual from committing future offences. In most cases that proposition appears to have been premised on the (not unreasonable) implied contention that extended retention of that material may assist in the identification of that individual if they commit offences in the future – and that the more likely one is to be detected if one commits an offence, the less likely one is to commit it. In

[39] See paragraph 124 of the Judgment of the ECtHR in *S & Marper v UK*.

some cases, however, it has also been contended – perhaps less convincingly – that the extended retention of a subject's biometric material may have a deterrent effect because it will demonstrate to that individual that the police will take a proactive approach to the prevention, detection and prosecution of any offences which he or she may commit in the future.

88. The weight that can properly be attached to the possibility that extended retention may have a 'deterrent' effect must, of course, turn on the particular circumstances of each case. Whereas it may well be an important factor in, for example, cases where there are grounds for concern that the subject may in the future become involved in violent crime against strangers, it is likely to be of very limited significance in, for example, cases where the subject appears unlikely to be able to exercise proper control over their future actions.

THE LIST OF QUALIFYING OFFENCES

89. In addition to its significance in the context of applications for extended retention, the question of whether or not an offence is a qualifying offence is of relevance to a number of other aspects of the current regime as regards the taking and retention of biometric material. The list of such offences appears at section 65A of PACE and that list was most recently expanded by *The Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013* which came into force on 11 November 2013.

90. It has been suggested that there are a number of surprising omissions from the current list of qualifying offences and, in particular, that that list should be further expanded so as to include offences such as:

- the possession of prohibited weapons (including firearms,[40] knives and other bladed articles); and
- the importation of Class A drugs and their possession with intent to supply.

In view of the seriousness of those offences – and in view of the fact that they are of a type in relation to which DNA and/or fingerprint evidence may well be of significance – I agree that that list might usefully be re-visited.

CONVICTIONS OUTSIDE ENGLAND AND WALES

GENERALLY

91. By sections 61(6D), 62(2A) and 63(3E) of PACE[41] the police have, with the authority of an officer of the rank of inspector or above, power to take fingerprints and a DNA sample from (broadly speaking) any person who has been convicted outside England and Wales of an

[40] The possession of a firearm alone is not a qualifying offence. Additional factors such as intention to endanger life or threaten violence (among others) must be present for the offence to count as a qualifying offence.

[41] (all inserted by section 3 Crime and Security Act 2010)

offence that would constitute a qualifying offence under the law of England and Wales. By section 63J of PACE[42] the police have the power to retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample.

92. Two issues have arisen in relation to these sections, one as regards the scope of section 63J and one as regards the practical operation of those sections as regards EU nationals who have been convicted abroad. Although only the latter was brought to my attention in the context of an application under section 63G, it is convenient to deal with both of them at this stage.

THE SCOPE OF SECTION 63J

93. Although section 63J allows the police to retain for an indefinite period biometric material which has been taken under sections 61(6D), 62(2A) or 63(3E), it has no application to biometric material that has been or is taken under any other section of PACE. Biometric material which has been or is taken under any other such section (e.g. when an individual is arrested on suspicion of having committed an offence) cannot lawfully be retained indefinitely simply because the individual in question has been convicted of a qualifying offence outside England and Wales. If the police wish to retain the biometric records of such individuals and have no other basis for doing so, they have no option but to go back to those individuals and to take further samples and fingerprints from them under those sections.

94. The effect of those legislative arrangements has been:

- that the DNA profiles and fingerprints of some thousands of individuals who have been convicted of such offences outside England and Wales have had to be deleted from the UK national databases; and
- that the police have been faced with the task of deciding whether or not it is appropriate to take further samples and fingerprints from those convicted individuals and, if so, of taking steps to do so.

It will be noted that, quite apart from the obvious resourcing and operational burdens that this involves for forces – and the possibility that some of the individuals in question may prove to be untraceable – it could reasonably be argued that re-arresting and re-sampling an individual following a conviction outside England and Wales constitutes a greater interference with their privacy than simply retaining biometric material which has already been obtained from them.

THE OPERATION OF SECTIONS 61(6D), 62(2A), 63(3E) AND 63J

95. EU Council Framework Decisions[43] detail the mechanisms for the exchange and use of foreign conviction information by EU member states. Where a UK national is convicted in

[42] (inserted by section 6 PoFA)

another member state, the relevant UK authorities will be notified of that fact and, if the offence is a recordable offence, the conviction will be recorded on the PNC. As regards the nationals of other member states who are present in the UK, however, information as to their conviction histories abroad will only be passed to the UK authorities in response to a specific request for such information. Such a request will usually be made for the purposes of criminal proceedings against the individual concerned and, broadly speaking, that information may only be used for those purposes[44] or *"for preventing an immediate and serious threat to public security"*.

96. As a general rule – and in view of the limited purposes for which it can be used – information about foreign convictions which is obtained in response to a request such as is referred to above is not, and cannot be, recorded on the PNC. However, in January of 2010 the Home Secretary approved a list of offences in relation to which an exception should be made to that general rule. That list was approved on the basis that individuals who had committed those offences would represent *"an immediate and serious threat to public security"*. Although those offences ('the listed offences') included a number of the more serious 'qualifying' offences, they by no means included all such offences.

97. It has been suggested to me by the police that as a result of:

- the limitations on the use to which foreign conviction information about EU nationals can be put; and/or
- the restricted circumstances in which the convictions of such nationals can be and are recorded on the PNC,

sections 61(6D), 62(2A), 63(3E) and 63J have proved to be of significantly less practical value than might reasonably have been expected. In particular, I have been informed that as a result of those factors the police have been and remain unable to take and retain under those sections biometric material from many EU nationals who they know to have been convicted of qualifying offences outside England and Wales.

98. This problem was raised with me in the context of an application under section 63G in respect of a (non-UK) EU national who had been arrested for, but not charged with, burglary. I was informed – and have no reason to doubt – that although enquiries of the relevant member state had established that he had served over 13 years imprisonment in that state for numerous similar offences, the above factors meant that it was not in practice open to the police to take and retain biometric material under those sections. Although I acceded to that application in respect of the material which had been taken when that individual was arrested, the relevant biometric records will, of course, be subject to a much

[43] 2009/315/JHA and 2009/316/JHA

[44] ("criminal proceedings" in this context are defined by Article 2(b) 2009/315/JHA as "the pre-trial stage, the trial stage itself and the execution of the conviction")

shorter retention period than would have applied if the police had been able to rely on those sections.

99. This seemed to me to be an obviously unsatisfactory state of affairs which might well be putting the UK public at unnecessary risk. I therefore raised it with Home Office officials and others and was told in August of 2014 that the list of offences that was issued by the Home Secretary in January of 2010 was at that time 'under review'. Although I have very recently been informed that changes have now been made to that list, I am as yet uncertain as to precisely how those changes will take effect or as to the extent to which they will prevent problems of this type arising in the future.

100. Whilst the problems which are discussed above have largely arisen in connection with non-UK nationals, it seems that difficulties have also arisen in connection with the taking and/or retention of biometric material from individuals who have been convicted of qualifying offences in Scotland or Northern Ireland. In particular I understand that, while in most cases of that type the biometric records of the individuals concerned will have been loaded to the relevant UK national databases (and will, under Scots or Northern Irish law, be subject to indefinite retention on those databases), in at least some cases:

- no DNA samples will have been taken from those individuals when they were convicted (and thus no DNA profiles will have been loaded to the National DNA Database); and
- technical issues associated with the operation of the PNC may make it impossible for forces in England and Wales later to procure the loading and retention of relevant DNA profiles pursuant to section 63J.

101. I understand that consideration is already being given to the possibility of seeking legislative changes to cater for at least some of these problems and, indeed, to allow police forces in England and Wales to take and retain biometric material from those who have been convicted elsewhere in the United Kingdom of any recordable offence (i.e. qualifying or non-qualifying). I will of course be keeping all these matters under careful review.

2.4 OTHER ISSUES ARISING AS REGARDS EXTENDED RETENTION

POLICE ENGAGEMENT WITH THE PROCESS

GENERALLY

102. As is pointed out above, by 31 August 2014 police forces had:

- made 91 applications to the Biometrics Commissioner under section 63G;
- given 32 Interim Notifications of possible future applications; and
- made 6 applications to District Judges under section 63F(7).

As is also pointed out above, save only for 3 of the applications under section 63G, all of those applications and Interim Notifications had been made or given by the MPS.

ENGAGEMENT BY THE MPS

103. From my dealings with the MPS it is apparent that it has engaged fully with the application process under section 63G and, indeed, with that under section 63F(7). It has established a Biometric Retention Unit with responsibility for such applications and that Unit has clearly done a great deal of work to identify cases where applications might be appropriate. As an indication of the scale of that work, I have been informed by the MPS that by 31 August 2014 it had involved consideration of some 28,000 cases in which individuals had been NFA'd for qualifying offences since 31 October 2013 and some 770 cases in which the 'automatic' three-year retention period in respect of individuals who had been charged with, but not convicted of, qualifying offences was due to expire on or after 31 January 2014.

104. It is worthy of note that, although I have been told by the MPS that in some 8,000 of those 28,000 'NFA' cases the individuals in question had no previous convictions, by 31 August 2014 the MPS had made applications under section 63G, or had given Interim Notifications, in only 123 of them i.e. in only about 1.5% of those 8,000 cases.[45]

ENGAGEMENT BY OTHER FORCES

105. There are a number of factors which may explain the relative scarcity of applications for extended retention from forces other than the MPS in the period to 31 August 2014. It seems likely, however, that an important part of that explanation has been the difficulty of identifying cases in which such applications might be appropriate and should be considered.

THE DIFFICULTY OF IDENTIFYING APPROPRIATE CASES

PNC ISSUES

106. The limitations of the PNC make it difficult for forces to identify cases in relation to which it may be appropriate for them to make applications for extended retention under section 63G i.e. cases in which someone without previous convictions has been arrested for, but not charged with, a qualifying offence.

107. In the absence of any easy means of identifying such cases – and as the MPS has found to its cost – forces who want to engage fully with the application process have limited options other than to embark on an elaborate and resource-intensive 'sifting' exercise so as:

[45] It is possible however, that in a significant number of those 8,000 cases it was open to the MPS to retain the relevant biometric material on some other basis (e.g. on the grounds that, since being NFA'd for the relevant qualifying offence, the individual in question had been arrested for, charged with, or convicted of some other offence).

- to identify all the cases in their areas in which an arrestee has been NFA'd for a qualifying offence; and
- then to exclude from that (sizeable) group of cases, all those in which the arrestee's biometric material can be retained otherwise than pursuant to an application to me (e.g. on the basis that they have some previous conviction or caution).

Similar difficulties arise as regards the identification of cases in relation to which it may be appropriate for forces to make applications for extended retention under section 63F(7).

108. At the Conference/Seminar which I held in June of this year I sought the views of force representatives as to this PNC issue and, in particular, as to the desirability of introducing a facility into the PNC whereby forces would be able to obtain reports which alert them to all the cases in their areas in which individuals without previous convictions have been NFA'd for qualifying offences (i.e. to all the cases in relation to which they might want to consider making applications for extended retention). Although I understand that other police representatives had previously expressed a different view, widespread support for the introduction of such a facility was expressed at that Conference/Seminar and in later correspondence.

109. At my suggestion it has now been agreed that such a facility will be introduced into the PNC: as yet, however, it is unclear when this will be done.

OTHER OPTIONS

110. Even in the absence of such a facility on the PNC or of an extensive 'sifting' exercise of the type that is undertaken by the Biometric Retention Unit of the MPS, it is, of course, open to forces to ensure that Investigating Officers are made aware of the scope for applications under section 63G – and that they are reminded to think about that matter (and if, appropriate, to follow it up with their SPOCs or otherwise) when they decide to NFA an arrestee for a qualifying offence. I have suggested to forces that they should adopt this course – most notably at my Conference/Seminar in June – and it is my impression that at least some forces are now actively pursuing it.[46]

THE RISKS OF NOT ENGAGING WITH THE APPLICATION PROCESS

111. There are at least two obvious risks associated with non-engagement by forces with the statutory processes whereby the normal retention periods for DNA profiles and fingerprints may be extended. The first is the resulting risk to public safety in that at least some crimes may go undetected or unprevented because those processes have not been utilised. The second is the reputational risk which forces run in that connection. Whatever may have been the position at an earlier stage, recent enquiries which have been made to my office

[46] I have been informed, moreover, that 2 forces have recently introduced processes which have made it easier for them to identify cases where applications under s.63G may be appropriate.

suggest that a number of forces have now recognised those risks and that at least some of them are now taking active steps to engage more fully with those processes. It will, of course, be easier – and cheaper – for them to do so if and when the proposed new facility on the PNC is introduced.

112. Other forces may, however, take a different approach.

113. It has been suggested to me that, in all the budgetary and other circumstances in which forces currently find themselves, the risks of non-engagement that are referred to above are reasonable ones for forces to run. As I understand it, the reasoning underlying that suggestion is (broadly speaking) as follows.

    i. Even if significantly more applications could sensibly be made under section 63G, the overall number of such applications will never be very substantial. Applications under that section should only be made – and will only be granted – in unusual and compelling circumstances. The MPS's experience to date suggests that, even if every force were to approach the application process in as rigorous and pro-active a manner as the MPS has done, only about 1,000 successful applications would be made every year.

    ii. Furthermore, of that 1,000 or so possible cases a year it seems unlikely that, even if some of the individuals concerned did go on to commit offences in the future, more than a handful would escape detection because their biometric records had not been retained. If, after all, those individuals did come under suspicion in the future, it would usually be possible for their DNA and fingerprints to be taken at that stage.

    iii. It is clear from the experience of the MPS that full and active engagement with the statutory processes as regards extended retention comes at a considerable financial price. It is at least arguable that the resources expended in that connection could more profitably be expended elsewhere. If, for example, a force identifies 50 or 100 people a year who, although they have no convictions, that force assesses as presenting a real risk to public safety, it is at least arguable that there are more cost-effective ways of reducing that risk than by expending time and resources on seeking to retain for an extended period those individuals' DNA profiles and/or fingerprints.

    iv. Against that background (so it has been argued) it is easy to justify non-engagement by forces with those statutory processes. In a world in which police budgets are constantly under strain – and where forces are every day having to make extremely difficult decisions as to the prioritisation of effort and expenditure – calculated risks have to be run and the risks of non-engagement which are referred to above are reasonable ones to run.

    Those contentions cannot in my view easily be dismissed.[47]

[47] It has also been suggested to me in this context:

THE PRACTICAL VALUE OF THE NEW PROCESSES

114. Given that it is only since 31 October 2013 that forces have been able to make applications under section 63G, and given the relatively small number of such applications that have been made since then, it is of course impossible to form any worthwhile view as to the actual or likely practical value of extended retention in the circumstances contemplated by that section.[48] It is clearly desirable that that issue be kept under close review and it is for that reason that, at my request, the Guidance issued by the NDNAD Strategy Board as regards applications under section 63G provides that:

> "*Individual Chief Officers will be required to maintain records in relation to any successful applications they make to the Biometrics Commissioner. The records must show what subsequent use has been made of the retained material, and any benefits in preventing and detecting crime which have resulted from that use*."

As is also recognised in that Guidance, however, it may well be difficult to quantify the extent to which the extended retention of an individual's biometric records has assisted in the detection of crime – and impossible to say whether (and, if so, to what extent) it has contributed to the prevention of crime.

115. I have investigated with academics and others the scope for research to be conducted in this regard and will continue to do so. On any view, however, it must be unlikely that, before the system has been in operation for at least 2 or 3 years, it will be possible to make a properly informed assessment of the practical value of extended retention in the circumstances contemplated by section 63G.

116. Whatever may prove to be the practical value of extended retention in those circumstances, the MPS has informed me of two practical benefits that have already flowed from the MPS's

---

(i) that police forces did not ask to be granted a right to make applications for 'discretionary' extended retention in the circumstances contemplated by s.63G (or, indeed, in those contemplated by s.63F(7));

(ii) that because such a right now exists, it is forces (rather than legislators) who largely bear the risks associated with the non-retention of biometric material in those circumstances; and

(iii) that in the view of at least some police officers that unrequested 'transfer of risk' is both unwelcome and unfair.

It has been pointed out, moreover:

- that under the 'Scottish model' there is no equivalent to the section 63G procedure (instead – and as is the position under PoFA in relation those without previous convictions who are arrested for, but not charged with, *non*-qualifying offences – the Scottish model adopts a 'brightline' rule as regards all those without previous convictions who are arrested but not charged i.e. no retention in any circumstances); and
- that although the Scottish model does allow the police to apply to the Sherriff Court for discretionary extensions to the automatic 3-year retention period that applies as regards those without previous convictions who are charged with, but not convicted of, certain sexual or violent offences, no such applications have, it seems, ever been made.

[48] The same is, of course, true as regards the practical value of extended retention in the circumstances contemplated by section 63F(7) (under which an application for extended retention can be made to a District Judge in respect of an individual who has been charged with, but not convicted of, a qualifying offence).

active engagement with the application process. Both arise out of its re-visiting in that context cases in which individuals have been NFA'd for qualifying offences.

i. In one of those cases (which involved an alleged sexual assault on a male under 13) it appeared to the MPS's Biometric Retention Unit that, on the evidence available, the individual in question should probably have been charged with the offence for which he had been arrested. That Unit therefore suggested that the decision to NFA him should be reviewed by the officer(s) in the case. This was done and, as a result of that review, it was decided that that individual should indeed be charged. He has since been convicted of that offence and his DNA profile and fingerprints can, of course, now be retained indefinitely.

ii. The other practical benefit identified by the MPS has been the identification of cases where, whether through oversight or otherwise, a DNA sample has not been taken – or a satisfactory DNA profile has not been derived – from an individual who has been arrested for a qualifying offence and then NFA'd. Such cases are, it seems, by no means unknown and in a number of them the officer in the case has, when alerted to the problem, been able to take – or re-take – a DNA sample at later stage.

The issue of absent or 'failed' DNA samples is one to which I return later in this report.

THE FUTURE

117. It seems possible, perhaps likely, that in the next year – and particularly if and when the proposed new facility on the PNC is introduced – more forces will engage more actively with the process for applications under section 63G and that the number of such applications will rise significantly. As is pointed out above, if the MPS and other forces were to make applications at a similar rate to that at which they were made by the MPS in July and August of 2014, the total number of applications per annum would be of the order of 1,200. If applications were to be made at that rate the casework required of my Office would, of course, be much greater than it has been to date and a number of changes to our internal processes would clearly be required.[49]

118. It is also possible, however, that at least some forces will instead conclude that, largely for the reasons suggested at paragraph 113 above, the risks of not engaging with the process for applications under section 63G – or, indeed, with the process for applications under section 63F(7) – are risks which it is reasonable for them to run given the budgetary and other pressures to which they are subject. Indeed, I understand that even in the MPS the future and funding of its Biometrics Retention Unit are being kept under constant review

[49] In particular, it would no longer be possible for me to give personal consideration to every application and – subject to the resources that were made available – it might well also be necessary to adopt a much less thorough approach to the examination of applications and supporting crime reports and statements, especially in cases where the arrestees in question chose not to make representations.

and that, at least in terms of personnel, the resources allocated to it have recently been substantially reduced.

119. No doubt Parliament will in due course wish to give further consideration to the statutory processes whereby the normal biometric retention periods which apply to those who have never been convicted of recordable offences can be extended at the discretion of the Biometrics Commissioner or a District Judge – and no doubt Parliament will be in a better position to do so once those processes have been in operation for a longer period and when further research has been conducted in relation to them.

3. NATIONAL SECURITY DETERMINATIONS AND RELATED MATTERS

3.1 STATUTORY BACKGROUND AND GUIDANCE AS TO NSDS

STATUTORY BACKGROUND

120. In addition to the powers to take DNA samples and fingerprints which are provided for in PACE, the police and other law enforcement agencies have the power to take such samples and prints pursuant to other legislation and, in particular, pursuant to:

- similar legislation applicable in Scotland and Northern Ireland; and
- the Terrorism Act 2000 ('TACT'), the Counter-Terrorism Act 2008 ('the CTA') and the Terrorism Prevention and Investigation Measures Act 2011 ('the TPIMs Act').

121. Until the introduction of the PoFA regime all such samples and fingerprints (and all DNA profiles derived from such samples) could, broadly speaking, be retained indefinitely on the grounds of national security whether or not the individuals in question were convicted of offences.

122. As well as introducing stricter rules as regards the retention by police in England and Wales of biometric material which has been obtained from unconvicted individuals pursuant to PACE, PoFA introduced stricter rules as regards the retention by police forces anywhere in the United Kingdom of biometric material which has been obtained from unconvicted individuals pursuant to TACT, the CTA or the TPIMs Act. It remains the case, however, that, in addition to their other retention powers, the police and other law enforcement authorities may retain DNA profiles and fingerprints for an extended period on national security grounds. They may only do so pursuant to a National Security Determination or 'NSD'.[50]

123. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[51] It must be in writing and, in England, Scotland and Wales, it has effect for a maximum of 2 years beginning with the date it is made. Although the statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different,[52] I understand that in practice the same 2-year maximum will be applied. An NSD may be renewed before its expiry for a further period of 2 years.

[50] NSDs may also cover *"relevant physical data"* i.e. (broadly speaking) palmprints and prints or impressions from other areas of skin: see section 18 of the Criminal Procedure (Scotland) Act 1995. In this section of my report the word 'fingerprints' should be read as including 'relevant physical data' as so defined.

[51] (i.e. the Chief Officer or Chief Constable of the force or authority that 'owns' the biometric records at issue)

[52] (i.e. that an NSD there has effect for a maximum of 2 years beginning with the date on which the relevant biometric material would have become liable for destruction if the NSD had not been made)

124. An NSD is only required if the material at issue cannot lawfully be retained on any other basis. It will, therefore, only be required where that material has been taken from an individual who has not been convicted of a recordable offence. An NSD should, moreover, only be made if the Chief Officer or Chief Constable is satisfied both:

- that its making is necessary in the circumstances of the particular case for the purposes of national security; and
- that the retention of the material is proportionate to the aim sought to be achieved.

125. NSDs may be made or renewed under:

(i) section 63M of the Police and Criminal Evidence Act 1984

(ii) paragraph 20E of Schedule 8 to the Terrorism Act 2000

(iii) section 18B of the Counter-Terrorism Act 2008

(iv) paragraph 11 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011

(v) section 18G of the Criminal Procedure (Scotland) Act 1995

and

(vi) paragraph 7 of Schedule 1 to PoFA.

A key part of the role of the Biometrics Commissioner is to keep under review every NSD that is made or renewed under those provisions. The Commissioner must also keep under review the uses to which material retained pursuant to an NSD is being put.

126. The Commissioner's responsibilities and powers as regards NSDs are set out at section 20(2) to (5) of PoFA. By virtue of those provisions:

- every person who makes or renews an NSD must within 28 days send to the Commissioner a copy of the determination and the reasons for making or renewing it;
- every such person must also disclose or provide to the Commissioner such documents and information as the Commissioner may require for the purposes of carrying out the review functions which are referred to above; and
- if on reviewing an NSD the Commissioner concludes that it is not necessary for any material retained pursuant to the determination to be so retained, the Commissioner may order the destruction of the material if it is not otherwise capable of being lawfully retained.

STATUTORY GUIDANCE

127. By section 22 of PoFA the Secretary of State must give guidance about the making or renewing of NSDs, and any person authorised to make or renew an NSD must have regard to that guidance. In the course of preparing or revising that guidance, the Secretary of State must consult the Biometrics Commissioner and the Lord Advocate.

128. In March of 2013 the Home Secretary launched a public consultation inviting views on draft Guidance that had been prepared in this connection.[53] The consultation opened on 26 March 2013 and closed on 20 May 2013. As a statutory consultee I provided a detailed written response to the consultation.[54] In that response I made the following (among other) observations.

- "*There are a number of ways in which the draft Guidance might more effectively achieve [its] stated objectives. To do so it should, in my view, provide more detailed guidance to those who are authorised to make or renew NSDs as to the principles upon which they should work – and as to the factors which they should take into account – when deciding whether or not to make or renew them. I also take the view that such Guidance should, if possible, include illustrative examples of situations in which the making of NSDs would – or would not – be appropriate*."

- "*No practical guidance is provided as to how [Chief Officers and Chief Constables] are to assess the issue of 'necessity' in any given set of circumstances,*[55] *nor as to the factors which they should take into account – or as to the approach they should adopt – when carrying out the balancing exercise which will be required of them*.[56] *As a result, the risk of inconsistency would seem to be a high one*."

- "*I respectfully agree with the suggestion [by James Brokenshire MP] that 'general principles and illustrative examples' would be valuable components of guidance about the making or renewing of NSDs*.[57] *In the absence of such components the current draft Guidance will, in my view, provide little practical assistance to those responsible for making NSDs and do little to inform or reassure the public as to the basis upon which biometric material is being retained*."

- "*Some clearer indication could, for example, presumably be given of what is meant by 'necessary' in this context (such as that it denotes something less than 'essential' but more than merely 'desirable' or 'useful') and it would presumably be possible to identify in general terms at least some of the factors which should be taken into account when considering the issues of 'necessity' and 'proportionality' (e.g. the nature, scale and immediacy of the relevant risk to national security, the cogency of the reasons for believing that retention may serve some useful*

[53] That draft Guidance can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170700/protection_of_freedoms_act_guidance.pdf

[54] A copy of that response can be found at https://www.gov.uk/government/publications/biometrics-commissioners-response-to-draft-guidance-on-national-security-determinations and a summary of all the responses can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/223679/Biometrics_Summary_of_consultation_responses.pdf

[55] The draft Guidance – like the final version – indicated that the Chief Officer or Chief Constable *"must believe that a NSD is necessary in the circumstances of the particular case for the purposes of national security"*.

[56] The draft Guidance indicated that the work of the Chief Officer or Chief Constable would *"involve balancing any interference with an individual's ECHR Article 8 rights against the need to retain ... material for national security purposes."* This passage was expanded in the final version.

[57] See paragraph 30 of the 18th Report of the JCHR at http://www.publications.parliament.uk/pa/jt201012/jtselect/jtrights/195/19502.htm

purpose, the lapse of time since the material was obtained, the age of the individual from whom it was obtained, etc)."

- "*To assist me in my general 'reviewing' role it would be helpful if ... information were retained and made available to me about the use to which retained material is put and about any benefits which result from that use. I assume that such material will repeatedly be 'searched against' and I would not require information about every such search; I am, however, concerned that statistical and other information should be retained and made available to me about any 'hits' on material which is covered by a NSD and about the practical benefits (if any) which flow from the retention of that material. I am also concerned that statistical and other information should be retained and made available to me about:*
    - *biometric material which is currently held for purposes associated with national security but in respect of which no application is made for a NSD (and which should therefore be destroyed unless otherwise capable of being lawfully retained); and*
    - *biometric material which is taken for such purposes (e.g. pursuant to Schedule 8 of the Terrorism Act 2000) but is not retained.*

  The draft Guidance would, in my view, be improved if it provided for the retention of such information and for its being made available to the Biometrics Commissioner."

129. Many of my points were taken into account in the final version of the Guidance which was issued in June 2013. However, no 'illustrative examples' were provided in that final version, apparently because:

    " ... through extensive discussions with the practitioner community it [was] not considered that the inclusion of illustrative examples would add to the effectiveness of the guidance and [their inclusion might] in some instances present operational risks."[58]

    I am not persuaded that it would be impossible to provide illustrative examples which would not present operational risks and remain of the view that the Guidance would be more useful if such examples were included.

130. A copy of the Guidance as issued can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf.
    I note that the section dealing with DNA samples requires updating to take account of changes introduced by section 146 of the Anti-social Behaviour, Crime and Policing Act.

[58] See page 1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/223679/Biometrics_Summary_of_consultation_responses.pdf

3.2 THE NSD PROCESS

GENERALLY

THE PROCESS

131. The NSD process is primarily one for Chief Officers.[59] It is to Chief Officers that applications for NSDs are made and it is Chief Officers who make or renew them. The Commissioner's role is a secondary one i.e. that of reviewing NSDs which Chief Officers have already made or renewed.

132. The Metropolitan Police Service (the MPS) plays a central role in counter-terrorism police work in the UK. Applications for NSDs are compiled and submitted to Chief Officers by the Joint Forensic Intelligence Team of the MPS (JFIT) or, in Northern Ireland, by the Police Service of Northern Ireland (PSNI). Those applications are then considered by Chief Officers and either approved or not approved by them.

133. Dedicated application software ('the NSD IT System') has been developed and made available to all stakeholders in the NSD process. That System runs on the police's National Secure Network to which my Office has access. If an application for an NSD is approved, the decision of the Chief Officer is recorded at the end of the application 'form' together with his or her reasons for approving the application. That document then becomes the NSD and the NSD IT System automatically forwards it to my Office for my review.

134. For obvious reasons, the subject of an NSD is not informed of its existence or of the information or reasons which led to it being made or renewed.

MY ENGAGEMENT WITH STAKEHOLDERS

135. I have had numerous meetings and other dealings about the NSD process – and about the national security aspects of my role more generally – with, or with representatives of, the following stakeholders:

- From within the Home Office, the Office for Security and Counter Terrorism (OSCT);
- From within the MPS:
  - the Director of Forensic Services;
  - JFIT; and
  - Counter Terrorism Forensic Services (CTFS), who are responsible for the CT databases;

[59] In this and subsequent sections the term 'Chief Officer(s)' denotes both Chief Officer(s) and Chief Constable(s) of Police, Provost Marshals of the Royal Navy, Royal Military or Royal Air Force Police Force, the Director General of the Serious Organised Crime Agency and the Commissioners for Her Majesty's Revenue and Customs.

- The Coordinator National Functions Counter Terrorism and others from the Association of Chief Police Officers, Terrorism and Allied Matters (ACPO TAM);
- The Security Service;
- PSNI, the Department of Justice for Northern Ireland, and the Northern Ireland Office;
- The Lord Advocate, the Crown Office and Procurator Fiscal Service, and Police Scotland.

136. I have also addressed a Seminar which was arranged by ACPO TAM for Special Branches, Counter Terrorism Units and others and I have contributed to guidance that ACPO TAM has issued to the National CT Network about the NSD process.

137. I am grateful to all those stakeholders for the courtesy and co-operation they have shown me. I am particularly grateful to them for that courtesy and co-operation in circumstances where there have been numerous other and more obviously pressing demands on their time. In general, I have been impressed by the helpful approach that has been taken by those with whom I have dealt, and by their recognition and acceptance that it is part of my function to ask difficult questions of them.

138. In my dealings with those stakeholders I have from the beginning made clear that there can, in my view, be no purpose in the NSD process which Parliament has introduced if it is to be nothing more than a mere 'tick box' exercise on the part of Chief Officers or myself – and that my own review function will be both impossible and worthless if the reasoning which lies behind the making of NSDs is wholly opaque and/or unexplained. In the main, those stakeholders have been quick to accept that proposition. They have also been quick to accept that applications for NSDs should provide as much detail as they reasonably can and that they should, in particular, provide sufficient relevant detail and information to enable a Chief Officer to make – and to enable me to be satisfied that he or she has made – a properly informed decision as to whether or not it is appropriate to make or renew an NSD in the particular circumstances of the case.

139. The most contentious issue that has arisen in the context of my dealings with those stakeholders has been that of striking an appropriate balance between:

    (i) the importance of my being provided with sufficient information to enable me properly to discharge my review function (as underpinned by the statutory obligation of Chief Officers to "*disclose or provide to the Commissioner such documents and information as the Commissioner may require for the carrying out of his functions*");[60] and

[60] See section 20(3)(b) of PoFA and paragraph 65 of the Statutory Guidance.

(ii) the need to take proper account of the extreme sensitivity of some intelligence material, of the 'need to know' principle, and of the desirability of reducing to a minimum the resource implications of the NSD process.

I am not yet fully convinced that the arrangements which have been arrived at strike such a balance and I intend to keep them under careful review. I am conscious that, once the process has been in operation for a year or so, they may need to be revisited in the light of practical experience.

PREPARATIONS FOR COMMENCEMENT

140. I had hoped that, as with applications under section 63G of PACE, I would be able to carry out a pilot exercise before the new NSD process came into operation on 31 October 2013. In the event this proved to be impossible due to IT and other issues. I was, however, able to examine proposed NSD applications (together with some of the underlying intelligence and other material) in connection with a number of individuals whose biometric records were currently being retained and to discuss them in detail with representatives of JFIT and of ACPO TAM. This process made it possible to identify and resolve a number of issues and was, I believe, of real assistance to all concerned.

141. In addition, I was taken in detail through a number of cases in which retained biometric records had in the past proved invaluable in the context of counter-terrorist operations and/or investigations.

APPLICATIONS FOR NSDS

SUBMITTING APPLICATIONS

142. As is explained above, applications for NSDs are compiled and submitted to Chief Officers by JFIT or, in Northern Ireland, by PSNI. This process involves JFIT or PSNI approaching forces, Counter Terrorism Units and others for intelligence, information and comments ('supporting data') about the individual whose biometric material is under consideration. That supporting data is then assessed by JFIT/PSNI and a decision is made as to whether or not to put an application for an NSD before the relevant Chief Officer. If it is decided that such an application should be made, the supporting data is summarised on the application form by JFIT and, where appropriate, 'sanitised' so as to take proper account of relevant sensitivities.

143. The Statutory Guidance issued by the Secretary of State states that officers who make applications for NSDs:

"… should set out all factors potentially relevant to the making or renewing of a NSD and their reasoned recommendation that the responsible Chief Officer or Chief Constable make or renew a NSD in the case at issue." [61]

JFIT/PSNI add such a 'reasoned recommendation' to the application form and the application is then submitted to the Chief Officer via the NSD IT System.

THE INFORMATION SUPPLIED TO THE CHIEF OFFICERS

144. It is, of course, for Chief Officers to decide what information they require when considering whether to make or renew NSDs. The final version of the Statutory Guidance states, however, as follows:

> *"45. The Chief Officer or Constable must carefully consider all relevant evidence in order to assess whether there are reasonable grounds for believing that retention is necessary for the purpose of national security. In doing so, they may wish to consider any or all of the following non-exhaustive categories of information:*
>
> *a) Police intelligence*
>
> *b) Arrest history*
>
> *c) Information provided by others concerned in the safeguarding of national security*
>
> *d) International intelligence*
>
> *e) Any other information considered relevant by the responsible Chief Officer or Chief Constable.*
>
> *46. The responsible Chief Officer or Chief Constable should also take into account factors including but not limited to the nature and scale of the threat to national security if the material is not retained and the potential benefit that would derive from the extended retention of the biometric material in question."*

Against that background (and as I have made clear to stakeholders) I would anticipate that a Chief Officer who is being asked to make or renew an NSD will expect to be provided with reasonably detailed information about the individual to whom the application relates, including intelligence and other information about his or her history, known activities, and relevant contacts with police, immigration and other authorities. In many cases it may also be appropriate for the Chief Officer to be provided with similar information about the individual's relevant associates and their activities and contacts with the authorities.

145. I would also anticipate, however, that Chief Officers will want to see more than a simple catalogue of historic facts and information about the individual and his or her associates. They will, I would expect, also want to be provided with a forward-looking analysis as to the nature of, and grounds for, existing and future concerns about the individual in question and with an explanation as to why it is believed that some genuinely

[61] See paragraph 56 of the Guidance. Paragraph 57 goes on to say (among other things): *"… The application should set out all relevant factors and considerations including those which may undermine the case for making or renewing a NSD."*

useful purpose will be served by the retention of their DNA profile or fingerprints. The NSD process is, after all, primarily one which looks to the future rather than to the past.

146. I made all these points to JFIT and others during the period that the new NSD process and its associated IT System were being developed and I have been impressed by the extent to which they have been adopted in practice.

THE MAKING AND RENEWING OF NSDS BY CHIEF OFFICERS

147. An NSD may only be made or renewed by a responsible Chief Officer or by his or her nominated deputy. That deputy must be of at least the rank of Assistant Chief Constable or Commander.

148. Chief Officers (or their deputies) must satisfy themselves – and must formally certify when they make or renew an NSD – that the retention of the material in question is in their view both 'necessary' and 'proportionate'. Although they are not routinely provided with the underlying intelligence and other information that is summarised in the application form, they may call for that and/or further information with a view to satisfying themselves that the application is truly reflective of the intelligence 'landscape' for the individual in question. Chief Officers record at the end of that form their reasons for making, renewing or refusing an NSD, some providing more detail than others.

From what I have seen to date it seems clear that Chief Officers and their deputies give careful consideration to applications for NSDs and that they will, on occasion, call for further information before they decide whether or not to approve an application.

THE COMMISSIONER'S ROLE

149. When an application for an NSD is decided by a Chief Officer, the NSD IT System automatically informs my Office and updates our 'task list' accordingly. If an NSD has been made or renewed, the application and the Chief Officer's reasons are reviewed by my Office and a reasoned recommendation is made as to what my decision should be. If appropriate, further information about the case may be sought at that or a later stage. Although it is the relevant Chief Officer who is statutorily obliged to provide me with documents and information, any requests for further information are, as a matter of practice, initially addressed to JFIT/PSNI.

150. Although I am obliged to keep under review every NSD that is made or renewed, it was always my hope and expectation that it would only be on relatively rare occasions that evidence which was sufficient to lead a Chief Officer to conclude that an NSD was appropriate would not also be sufficient to lead me to conclude that it was right to make that NSD and that it was right that the material in question be retained. As I made clear at an early stage, however, if I was to add significant 'value' to the operation of the NSD process as well as to its establishment, it was inevitable that, during at least the first few

months of its operation, I would quite often want to look behind the summarised information on NSD application forms and seek details of the underlying intelligence.

151. The NSD IT System does not allow me or my Office automatic access to all the underlying information and documentation that is referred to in an application for an NSD. It is therefore necessary for us specifically to ask JFIT to grant us access to that information and documentation in cases where we want to see it. Although JFIT have been more than co-operative in that connection, this arrangement seems unnecessarily labour-intensive and time-consuming.

152. My Office has sought and obtained further information on specific points as regards a number of the NSDs that have been made and approved since the process came into operation. We have earmarked others for a future 'dip sampling' exercise during which we will seek to examine:

- the underlying information and documentation that is referred to in the relevant applications; and/or
- additional information and documentation about any developments since the dates on which the NSDs were made.

153. Although my principal statutory functions as regards NSDs are those of *"keeping under review"* every NSD that is made or renewed and *"the uses to which material retained pursuant to … [an NSD] … is being put"*, at section 20(4) and (5) of PoFA it is provided that:

> "*If, on reviewing a national security determination … the Commissioner concludes that it is not necessary for any material retained pursuant to the determination to be so retained, the Commissioner may order the destruction of the material if … the material … is not otherwise capable of being lawfully retained.*"

This is a striking power and it is clearly not one that I can properly exercise merely because I am not persuaded that an NSD has been properly made and/or that the continued retention of the material at issue is both necessary and proportionate. In particular, it must clearly be possible that there will be times when, perhaps because of the insufficiency of the underlying information, I am *neither* satisfied that an NSD has been properly made *nor* able to conclude that it is unnecessary for the material to be retained.[62]

154. In reality, then, I have at least three options when reviewing an NSD:

(i) I can 'approve' the NSD – a decision that will be appropriate if I am satisfied that the retention of the biometric material is necessary and proportionate in the interests of national security.

[62] Indeed – and given that PoFA provides that, even if the Commissioner does conclude that it is not necessary for material to be retained, the Commissioner *"may"* (rather than *"must"*) order its destruction – there may presumably be times when, although I feel able to conclude that it is not necessary for the relevant material to be retained, I am not persuaded that it would be right to order its destruction.

(ii) I can 'not approve' the NSD but make no order for the destruction of the relevant material – a decision that will be appropriate where, on the information provided:

- I am not satisfied that retention of the biometric material is necessary and proportionate in the interests of national security

but equally

- I cannot, on the information provided, safely conclude that it is not necessary for the material to be retained and that it should be destroyed.

(iii) I can 'not approve' the NSD and also conclude that it is not necessary for the relevant material to be retained and that it should be destroyed.

The NSD IT System provides for all three of those options. It also assumes, I think sensibly, that I will not take the second or third of those courses without first giving the relevant Chief Officer/JFIT an opportunity to present further evidence and/or argument to me.

IMPLEMENTATION AND NUMBERS

LEGACY MATERIAL AND NEW MATERIAL

155. NSDs may be made in respect of 2 categories of material:

- 'Legacy Material' (i.e. material taken under relevant statutory powers *before* the relevant provisions of PoFA came into effect on 31 October 2013); and
- 'New Material' (i.e. material taken under such powers *after* that date).

156. Until 31 October 2013 – and as has been pointed above – Legacy Material had generally been subject to indefinite retention on the grounds of national security whether or not the individual in question was convicted of an offence. By section 25 of PoFA the Secretary of State was required to make an order prescribing appropriate transitional procedures as regards Legacy Material and by such an Order[63] the police and relevant law enforcement agencies were given two years (i.e. until 31 October 2015) to assess that material and to decide whether or not to apply for NSDs in relation to it. In practice, then, since 31 October 2013 Legacy Material which cannot otherwise lawfully be retained has been subject to a maximum retention period of 2 years unless an NSD is made in respect of it. If an NSD is made in relation to such Legacy Material before 31 October 2015, that material may be retained for the period that that NSD has effect.

157. For New Material, the retention period which applies in the absence of an NSD of course depends upon the legislation governing the powers under which it was taken. As regards material which has been taken under counter-terrorist legislation from individuals who have

[63] The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) Order 2013 No.1813 (http://www.legislation.gov.uk/uksi/2013/1813/contents/made)

been arrested or detained without charge, the relevant retention periods in the absence of an NSD can be summarised in schematic form as follows:

Provision	Relevant Material	Retention Period*
Paragraph 20B Terrorism Act 2000 (TACT)	DNA profiles/fingerprints relating to persons detained under s.41 TACT.	3 years
Paragraph 20C Terrorism Act 2000 (TACT)	DNA profiles/fingerprints relating to persons detained under sch.7 TACT.	6 months
Paragraph 20(G)(4) Terrorism Act 2000 (TACT)	DNA samples taken under TACT.	6 months (or until a profile is derived if sooner). May be kept longer if required under CPIA.
Paragraph 20(G)(9) Terrorism Act 2000 (TACT)	DNA samples relating to persons detained under s.41 TACT.	6 months plus 12 months extension (renewable) on application to a District Judge (Magistrates Court). May be kept longer if required under CPIA.
S.18 Counter-Terrorism Act 2008	S.18 DNA samples	6 months (or until a profile is derived if sooner). May be kept longer if required under CPIA.
S.18A Counter-Terrorism Act 2008	S.18 CTA DNA profiles/fingerprints.	3 years
Schedule 6, Paragraph 12 Terrorism Prevention and Investigation Measures Act 2011	DNA samples Relevant physical data (Scotland)	6 months (or until a profile is derived if sooner). May be kept longer if required under CPIA.
Schedule 6, Paragraph 8 Terrorism Prevention and Investigation Measures Act 2011 (TPIM)	DNA profiles/fingerprints taken under Sch.6, paras.1 and 4 of TPIM.	6 months beginning with the date on which the relevant TPIM notice ceases to be in force. If a TPIM order is quashed on appeal, the material may be kept until there is no further possibility of appeal against the notice or decision.

*The retention period starts from the date the relevant DNA sample/fingerprints were taken unless otherwise stated.

ASSESSMENT OF LEGACY MATERIAL

158. A great deal of work has been done – and continues to be done – assessing Legacy Material that is being held for national security purposes with a view to establishing:

- whether or not it will be lawful to continue holding it after 31 October 2015 if no NSD has been made in the meantime

and, if not,

- whether an NSD should be applied for in respect of it.

Although that assessment work is much less far advanced than might have been hoped, substantial progress has now been made.

159. I have made various visits to JFIT and CTFS during which we have discussed this assessment work. I have been shown the systems used and have had the relevant processes explained to me. I have also done some dip-sampling of biometric records that are being held on the grounds of national security. I am satisfied that this assessment work is being done properly and with care and that Legacy Material that falls within the ambit of the new PoFA regime has been – and is being – handled appropriately.

160. It is possible that, given the way in which the new regime has been introduced, Legacy Material may lawfully be retained until 31 October 2015 even in circumstances where:

- it has been specifically decided not to apply for an NSD in respect of that material; or
- such an application has been made and rejected by the relevant Chief Officer; or
- an NSD has been made in respect of that material but I have decided that it is not necessary for that material to be retained and that it should be destroyed.

I understand, however, that in those circumstances it has been and will be normal practice for the relevant material to be destroyed as soon as reasonably possible after the completion of the assessment or NSD procedure in respect of it. I have sought and obtained confirmation of the destruction of such material and shall continue to do so in the future.

HANDLING OF NEW MATERIAL

161. I am likewise satisfied that, as regards New Material, assessment work is being done properly and with care and that that material is being handled appropriately. I have recently been informed, however, that as a result of delays in the handling of such material and/or in the provision of information to CTFS and JFIT, it is possible that a small quantity of New Material which could and should have been made subject to NSDs before the relevant statutory retention periods expired will in fact have to be deleted. I am making urgent enquiries into this matter but understand that steps have already been taken to reduce the risk of any such delays in the future.

NUMBERS

162. It has been suggested to me that it would be contrary to the interests of national security for me to disclose the number of individuals whose DNA profiles or fingerprints are currently being held by the police or other law enforcement authorities for national security purposes. It has also been suggested that it would be contrary to the interests of national security for me to disclose the number of NSDs that have been made or the number that I have reviewed. Although I am not wholly persuaded that either of those suggestions is correct – or that, if they are, that will inevitably remain the case in future years – I see no reason to believe that any very useful purpose would be served by the disclosure of that information at this stage and I have therefore decided that it is, on balance, appropriate for me to proceed on those assumptions for the purposes of this present report. I will, however, keep this issue under close review in future years.

OBSERVATIONS

I am satisfied, however, that I can properly disclose at least the following information.

i. I had expected to receive NSDs for review from the beginning of November 2013 i.e. shortly after the commencement of PoFA. In the event, however, the first NSD received in my office was received on 2 May 2014.

ii. A number of factors have contributed to the slow implementation of the NSD process. Although those factors have, it seems now been addressed, I shall of course keep the situation under careful review. As I have indicated above, I am also taking urgent steps to establish whether (and, if so, to what extent) those delays have had practical consequences to the possible detriment of national security.

iii. The NSD IT System allows me access not only to NSD applications that are approved by Chief Officers but also to those that are not. All the application forms that I have seen have set out detailed information and reasoning and it seems clear that Chief Officers have given careful consideration to those applications before deciding whether or not to approve them.

iv. I have also been provided with detailed information about a number of cases in which it has been decided that NSDs should not be applied for in connection with Legacy Material. From those cases it is in my view clear that sensible judgment is being exercised as to whether or not there are good grounds for making such applications.

v. As at 31 August 2014 I had had no cause to overturn a decision of a Chief Officer in relation to an NSD.

vi. Given:

- the quantity of the Legacy Material and the discussions about it that I have had with stakeholders;

- that the police and law enforcement agencies have only 2 years from 31 October 2013 to assess the entirety of that material and, where appropriate, to procure the making of NSDs in respect of it;
- that 6 months of that period had elapsed before the first NSD was received for review in my Office; and
- that relatively few NSDs have been received by my Office since then,

I have some concerns about the demands which will be made on my Office – and about the resources which it will require – if I am properly and promptly to review all the NSDs which seem likely to be made before 31 October 2015.

vii. More importantly, in the light of those and other factors I have real concerns as to whether it will be possible for JFIT/PSNI to complete by 31 October 2015 their assessment of the Legacy Material and to procure that all the NSDs that should by that time be made in respect of that material are in fact made.

viii. In the context of the establishment of the NSD process it has been necessary for various stakeholders to review and refine their processes and for JFIT/PSNI to 'pull together' and review the information about relevant individuals that is held by forces, Counter Terrorism Units and others. The taking of such steps can only have been to the benefit of national security. Other (and more tangible) benefits to national security which have flowed from the introduction of the new biometric retention regime are referred to below.

THE USES TO WHICH NSD MATERIAL IS BEING PUT

163. As well as keeping under review every NSD that is made or renewed, I must also keep under review the uses to which material retained pursuant to an NSD is being put. I have nothing of substance to report in that latter regard save only that I have seen nothing to suggest that that material is being used otherwise than for permitted purposes.

164. Given the short period during which the new NSD process has been in operation it is impossible to form any worthwhile view as to the actual or likely practical value of extended retention of biometric material pursuant to NSDs. Although I intend to keep that issue under close review, it must be unlikely that it will be possible to form or express any such view until the system has been in operation for at least 2 or 3 years.

3.3 OTHER MATTERS RELATING TO 'NATIONAL SECURITY' HOLDINGS OF MATERIAL

OVERSIGHT FUNCTION

165. By section 20(6)(a) to (d) of PoFA I have the function of keeping under review the retention and use of DNA samples, DNA profiles and fingerprints in accordance with specified

provisions of PACE, TACT, the CTA and the TPIMs Act. I also have the function of keeping under review the retention and use of copies of those profiles and prints. I deal later in this report with my general oversight function as regards biometric material that is taken and used for normal policing purposes: it is convenient, however, to deal in this section of my report with my general oversight function insofar as it relates to counter-terrorism matters. It will be noted that in that connection my oversight function is concerned only with material that falls within the ambit of those provisions and that it does not, for example, cover material that is held for national security purposes by the Armed Forces or by the Security Service.

DNA SAMPLES

166. In England, Wales and Northern Ireland the destruction regime for DNA samples taken under the relevant provisions of TACT, the CTA and the TPIMs Act is broadly similar to that prescribed under PACE. As a general proposition any DNA sample taken on detention or arrest must be destroyed as soon as a profile has been derived from it and in any event within six months of the date it was taken. In Scotland, however, different rules apply and, unlike the position elsewhere, a DNA sample may (like a DNA profile or fingerprints) be the subject of an NSD.

167. I have seen nothing to suggest that DNA samples taken pursuant to those provisions have been retained beyond the permitted timescales or have been used otherwise than for permitted purposes. Nor have I seen anything to suggest that, in the context of counter-terrorism matters, DNA samples taken under any other provisions have been unlawfully retained or used.

DNA PROFILES AND FINGERPRINTS

168. The CT DNA Database is a standalone database of CT-related DNA profiles and crime scene stains. It is operated solely by CTFS. The CT Fingerprint Database is a separate and secure database within IDENT1 for CT-related fingerprints and crime scene fingermarks. It is also operated solely by CTFS.

169. As I have indicated above, I have decided that for the purposes of this present report it is appropriate for me to proceed on the assumption that, as has been suggested to me, it would be contrary to the interests of national security for me to disclose the numbers or sources of the biometric records on these CT databases. I am satisfied, however, that I can properly make the following points.

    i. As I have mentioned above, I have made various visits to JFIT and CTFS and I have done some dip-sampling of the biometric records that are being held on the CT databases. Insofar as those fall within the ambit of the new PoFA regime, I am satisfied that they are being handled appropriately and I have seen nothing to suggest that that they – or that copies of them – are being retained or used

otherwise than in accordance with the relevant statutory provisions. These are, of course, matters which I intend to keep under careful review.

ii. I have taken a particular interest in the arrangements whereby CT-related biometric records may be shared with (or, indeed, obtained from) foreign or international law enforcement agencies and/or other UK government agencies. In that connection – and as well as discussing those matters with stakeholders – I have examined various agreements and MOUs between the MPS and such agencies and, having done so, I have seen nothing that has caused me concern as regards the sharing of such records. Once again, however, this is a matter which I intend to keep under careful review.

iii. As stakeholders have been quick to agree, it is clear that the CT databases have evolved without there being in place the sort of comprehensive and clearly documented governance arrangements, policies and protocols that one might reasonably expect.[64] I have seen nothing to suggest that this 'governance deficit' has given rise to impropriety and recognise that that 'deficit' is perhaps unsurprising given the pressures under which those involved have been working and the need to prioritise casework over process. In any event, however, I am satisfied that the relevant stakeholders now recognise that it is important that proper governance arrangements and documentation be put in place as quickly as possible and I shall continue to work with them to that end.

CROSS-SEARCHING OF DATABASES

BACKGROUND

170. In order to comply with PoFA, it was necessary for approximately 1.8 million DNA profiles and approximately 1.7 million fingerprint records to be deleted from the national databases before commencement in October 2013. Before those deletions took place, permission was granted by ministers for counter-terrorism police to undertake a comprehensive 'cross-searching' exercise so as to ensure that the CT databases were up-to-date and that potential matches were not lost.

[64] At paragraph 8.1(b) of the Governance Rules of the NDNAD Strategy Board, however, it is expressly provided that that Board has responsibility for "*the oversight of the scientific operation of the Counter Terrorism DNA Database*": see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/320005/9781474106412_WEB.pdf

DNA PROFILES

171. Previous cross-searching between the national and CT DNA databases had been done on an *ad hoc* basis. In anticipation of the coming into force of PoFA and the mass deletion of profiles from the NDNAD, however, CTFS were in January of 2013 provided with an electronic copy of the complete NDNAD dataset of subject and crime scene profiles in order to 'wash through' that dataset against the CT DNA Database and to search for matches between the profiles on those databases. Further copy datasets were provided to CTFS for the same purpose before each of the pre-commencement 'bulk' deletions of profiles from the national database. I have been assured – and see no reason to doubt – that each of those copy datasets was subsequently destroyed, that the relevant biometric data was not shared with any third party, and that that data was used solely for the purpose of this cross-searching exercise.

172. In January of 2014 a long-term facility was put in place whereby profiles loaded to the National DNA Database can be and are 'washed through' against the CT DNA database. This arrangement is governed by a Data Interchange Agreement between the Home Office and the MPS which imposes clear restrictions on the use that can be made of those profiles and on the length of time for which they can be retained. I understand that in practice they are deleted from the CT database within two weeks of being loaded to it.

FINGERPRINTS

173. Since 2012 all new ten-print fingerprint sets loaded to IDENT1 have been automatically washed through the CT Fingerprint Database. In preparation for the commencement of PoFA, however, a comprehensive cross-searching exercise was undertaken whereby all the unidentified crime scene fingermarks on the CT database from UK operations were checked against IDENT1 before the 'bulk' deletions necessitated by PoFA took place.

RESULTS

174. I have been told that these cross-searches of DNA profiles and fingerprints generated a significant number of possible matches which were then assessed, and that a significant number of 'identifications' resulted. I understand, moreover, that many of those 'identifications' might never have been made but for the need to delete biometric data pursuant to PoFA and the impetus that gave to the introduction of more efficient cross-searching facilities.

4. THE DESTRUCTION AND/OR DELETION OF BIOMETRIC MATERIAL

4.1 DNA SAMPLES

BACKGROUND

175. As regards DNA samples (and as has been pointed out earlier in this report) the general rule provided for in PoFA is that any DNA sample that is taken in connection with the investigation of an offence must be destroyed as soon as a profile has been derived from it and in any event within six months of the date it was taken.[65] That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.

176. On 13 December 2012 Lord Taylor of Holbeach CBE laid a Written Ministerial Statement before Parliament. In it he said:

> *"Before the Act commences, it is necessary to destroy a significant amount of existing biometric material that the Act would not allow to be retained.*
>
> *The first priority is the destruction of DNA samples. A DNA sample is an individual's biological material, containing all of their genetic information. The Government does not want to retain the complete genetic makeup of any of its citizens. Every DNA sample taken will be destroyed as soon as a DNA profile for use on the database has been obtained from it. Destruction of existing DNA samples will begin in December 2012 and be completed by May 2013."*

On 24 October 2013 Lord Taylor and James Brokenshire MP laid a further Written Ministerial Statement before Parliament in which they stated that "*7,753,000 DNA samples containing sensitive personal biological material, no longer needed as a DNA profile has been obtained, have been destroyed.*"

177. In view of the significance of the genetic information which is contained in DNA samples – and the widespread concern that was expressed about information of that type becoming and/or remaining available to the police – I have taken a particular interest in the development and implementation of the new rules as regards sample destruction and in the steps that have been taken to ensure that DNA samples have been and are only retained in circumstances where that retention is lawful.

THE 'CPIA EXCEPTION'

178. Under the retention regime provided for by PoFA, the only situation in which the police are entitled to retain a DNA sample for more than six months is where:

(i) the sample was taken from an individual in connection with the investigation of a 'qualifying' offence; and

[65] See section 63R of PACE as inserted by section 14 of PoFA.

(ii) the police can satisfy a District Judge that that sample is likely to be needed in proceedings for the offence for the purposes of:

(a) disclosure to, or use by, a defendant; or

(b) responding to any challenge by a defendant in relation to the admissibility of material that is evidence on which the prosecution proposes to rely.

In those circumstances a District Judge may make a (renewable) order ('a deferred destruction order') whereby the DNA sample can be retained for a period of 12 months from the date on which that sample would otherwise have to be destroyed. That sample must not be used otherwise than for the purposes of any proceedings for the offence in connection with which the sample was taken.[66]

179. Even before PoFA came into effect, however, it was suggested that a wider exception to the 'six-month rule' was required and that, as is provided for in PoFA in relation to DNA profiles and fingerprints, the police should be entitled to retain any DNA sample beyond what would otherwise be its maximum retention date if it:

"is, or may become, disclosable under –

(a) the Criminal Procedure and Investigations Act 1996; or

(b) a code of practice prepared under section 23 of that Act and in operation by virtue of an order under section 25 of that Act."

Put shortly, that 1996 Act ('the CPIA') governs the gathering, use and retention of evidence during and after criminal investigations and the disclosure requirements as regards such evidence. A striking aspect of the relevant provisions of PoFA[67] was that DNA samples – and, indeed, any other samples taken under Part V of PACE[68] – were specifically excluded from the 'CPIA exception' that applied as regards DNA profiles and fingerprints.

180. A variety of arguments were put forward in support of the suggestion that the CPIA exception as regards DNA profiles and fingerprints should be extended to cover DNA and other samples. Some of those arguments seemed to me to be of questionable force and I had extensive discussions about that suggestion with Home Office officials. Among the possibilities that were canvassed during those discussions was the possibility that, if the CPIA exception were extended to cover DNA samples, it should expressly be provided:

- that, like a DNA sample covered by a 'deferred destruction order', any DNA sample retained pursuant to that exception must only be used for the purposes of any proceedings for the offence in connection with which that sample was taken; and
- that once a DNA sample ceases to fall within that exception, it should immediately be destroyed if the time specified in PACE for its destruction has already passed.

[66] See sections 63R and 63U(5) of PACE as they are set out at sections 14 and 17 of PoFA.

[67] (i.e. sections 14 and 17)

[68] (such as samples of blood or urine)

In the event, provisions to that effect were included in the further amendments to PACE[69] by which a CPIA exception was introduced as regards DNA samples. Those amendments were made by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014 and came into force on 13 May 2014. In the period between 31 October 2013 and 13 May 2014 the PoFA provisions governing sample destruction took effect as if the original CPIA exception applied to samples as well as to profiles and fingerprints.[70]

181. In October of 2013 – and while the proposed 2014 Act was undergoing legislative scrutiny – the Joint Committee on Human Rights ('the JCHR') issued a report[71] in which it made the follow observation as regards the application of the CPIA exception to DNA samples.

> *"188. We note the Bill's proposed safeguards in relation to the retention of samples. We recommend the following additional safeguards to protect against the prolonged retention of samples, particularly on a precautionary or speculative basis:*
>
> - *a robust process is established to ensure that each sample is considered and a determination is made as to whether or not it is required for the purposes of the CPIA. If it is not required, it should be destroyed within the PACE time limits.*
> - *a robust independent audit regime of retained samples under CPIA is established to help ensure against unnecessary prolonged retention. HMIC or ICO could carry out this function. ..."*

182. The Government agreed those recommendations. In its reply to the JCHR report [72] it made the following observations.

> *"... For DNA samples, police forces have been advised that under the regime created by the amendment, the norm will be that samples taken for DNA analysis will be destroyed by forensic suppliers after processing to produce a DNA profile. The advice also states that, should forces require the retention of the sample for casework purposes, they will need to notify the forensic supplier at the time of submitting the sample for analysis, and this is only to be done when a forensic scientist is carrying out an expert comparison of DNA evidence, not in the case of routine DNA matches from the National DNA Database.*
>
> *We agree that independent oversight of sample retention is required. This is the role of the Biometrics Commissioner – section 20(6) of the Protection of Freedoms Act 2012 requires him to keep under review the retention and use of fingerprints, DNA profiles and samples under the Police and Criminal Evidence Act. The Commissioner had already raised the need for particularly careful oversight of sample retention in the context of the CPIA and discussions are being held with him about the details of his role in this connection and the information he will need to carry it out."*

---

[69] (and, indeed, to TACT)

[70] See The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) Order 2013 at http://www.legislation.gov.uk/uksi/2013/1813/contents/made

[71] See http://www.publications.parliament.uk/pa/jt201314/jtselect/jtrights/56/56.pdf

[72] See http://www.parliament.uk/documents/joint-committees/human-rights/Letter_from_Norman_Baker_MP_111113.pdf

These discussions have largely been with the Head of the NDNAD Delivery Unit ('the NDU') and I deal with their upshot below.

HAVE SAMPLES BEEN APPROPRIATELY DESTROYED?

GENERALLY

183. Both before and after the commencement of PoFA the great bulk of DNA samples taken by the police have been processed by – and, if retained, have been retained on behalf of the police by – three independent Forensic Science Providers ('FSPs').[73] I have visited each of those FSPs – one of them on two occasions – to learn about and inspect, among other things, the destruction processes and policies they have followed as regards DNA samples and the deletion and 'de-linking' processes and policies they have followed as regards DNA profiles.[74] I have found no reason to doubt the accuracy of the pre-commencement sample destruction figure of 7,753,000 which was given in the Written Ministerial Statement of 24 October 2013. I have also found no reason to suspect that since that date (and save only in reliance on the CPIA exception to which I return below) significant numbers of DNA samples have been retained after profiles have been derived from them or for more than six months after the date they were taken.

184. In this connection three points merit particular mention.

i. The costs associated with the storage of millions of DNA samples were substantial and neither FSPs nor police forces had or have a significant commercial incentive to store large numbers of samples which could and should be destroyed. In those circumstances – and quite apart from the legal, reputational and other risks that would have been involved if they had continued to hold samples when it was unlawful for them to do so – it would perhaps be surprising if FSPs or forces had deliberately chosen not to comply with the new retention/destruction regime.

ii. All independent FSPs are subject to regular independent assessment and 'auditing' by the United Kingdom Accreditation Service ('UKAS'). Following a joint proposal by the Head of the NDU and myself it has recently been agreed by the Home Office that, as part of UKAS's work in relation to FSPs, UKAS will carry out detailed 'PoFA compliance checks' so as to obtain assurance as to, among other things, FSPs' past and present performance and processes as regards the destruction of DNA samples. Detailed 'scoping' work has already been done in this connection by UKAS and the NDU and I am very grateful to them for that work.

iii. Although I had hoped that it would also be possible for UKAS to carry out similar 'PoFA compliance checks' on police forces, it seems that there would be procedural

[73] They are Orchid Cellmark Limited, LGC Limited and Key Forensic Services Limited.

[74] See footnote 84.

and other difficulties with such an arrangement. I therefore intend to carry out compliance checks on police forces myself, probably in tandem with checks as regards the retention of DNA samples in reliance on the CPIA exception. I have already carried out one 'compliance check' in relation to samples which were being retained by Thames Valley Police and found nothing to suggest that the relevant retention rules were being breached.

THE CPIA EXCEPTION

NUMBERS

185. DNA samples which are retained pursuant to the CPIA exception may be either:

- samples taken from arrestees (known as 'arrestee', 'PACE' or 'reference' samples); or
- samples taken from – and with the consent of – third parties in connection with the investigation of an offence (known as 'elimination' or 'volunteer' samples).

I have been closely monitoring the numbers of such samples that are being retained pursuant to that exception.

186. To assist me in that connection the NDU has provided me with monthly schedules based on returns made by FSPs and police forces. The figures given in those schedules include both arrestee samples and elimination samples and the relevant figures are (so far as is possible) broken down by force. Each month those schedules provide the numbers of such samples that are being held by FSPs on behalf of forces; every three months those schedules also provide details of the numbers of such samples that are being held 'in force'.

187. Unfortunately – and largely, it seems, because of administrative and/or resource difficulties – by no means all forces have provided returns to the NDU in relation to their 'in force' holdings and in those circumstances the figures which appear below are incomplete.[75] It should also be noted that the schedules which have been provided to me almost certainly include a (relatively small) number of samples that are being retained otherwise than pursuant to the CPIA exception in that they are samples which have not been taken in connection with the investigation of an offence[76] and/or in that they are being retained by an FSP on behalf of forces from outside England and Wales.

188. Subject to those caveats, however, it seems likely from the figures which have been provided to me that as at 31 August 2014 a total of approximately 19,200 DNA samples were being retained by FSPs and forces pursuant to the CPIA exception. Of that number:

- some 1,260 were arrestee samples and some 17,940 were elimination samples; and

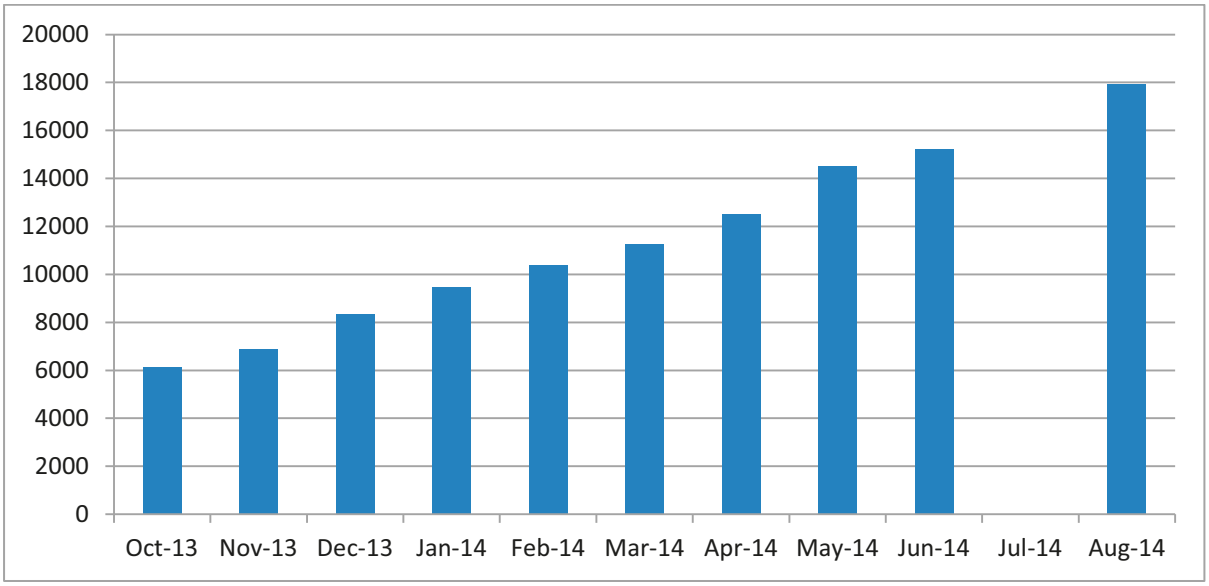
[75] The NDU and I have raised this problem with the defaulting forces and will of course pursue it with them if their returns remain incomplete.

[76] (e.g. samples from 'vulnerable persons' which are loaded to the Vulnerable Persons DNA Database).

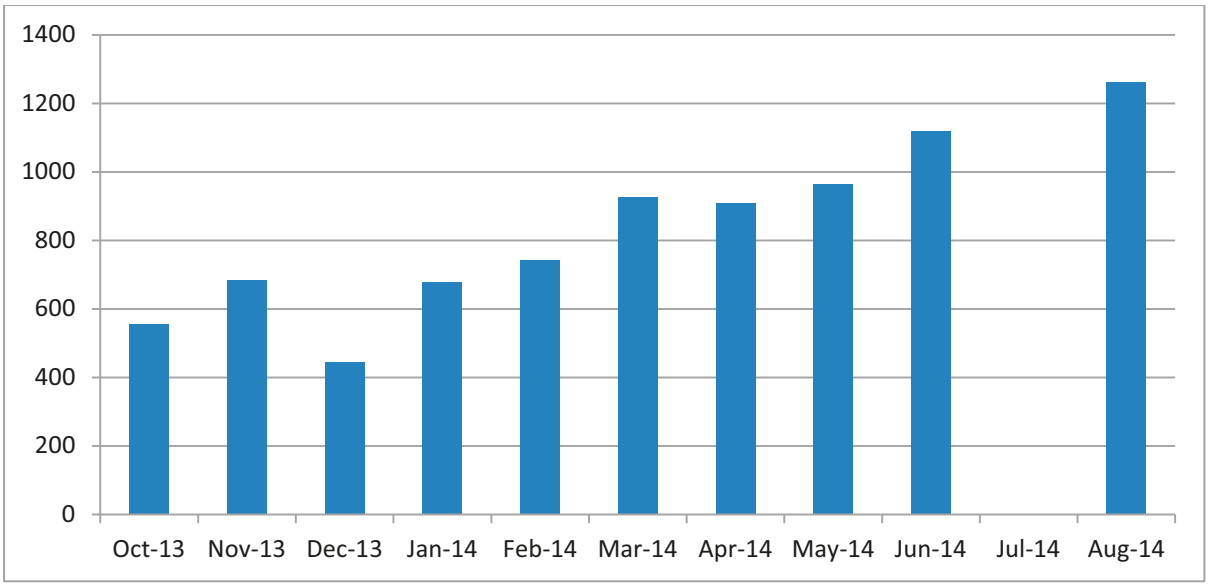
- some 18,780 were being held by FSPs and some 420 were being held 'in force'.

189. The following charts show how these retention figures have changed in the period 31 October 2013 to 31 August 2014.[77]

SAMPLES RETAINED UNDER CPIA (ELIMINATION)



SAMPLES RETAINED UNDER CPIA (ARRESTEES)



ELIMINATION SAMPLES

190. I understand that, since August of 2013 and unless specifically instructed otherwise, FSPs have been retaining until further notice all elimination samples that have been submitted to them. The consequence of this policy appears to have been that, of the DNA samples that have been taken in connection with the investigation of offences since August of 2013:

[77] Figures for July 2014 were unavailable because one of the FSPs was unable to supply data for that month.

- only a very small proportion of those that were taken from people who were suspected of having committed those offences (and who may, indeed, have gone on to be convicted of them) have been retained beyond the time specified for their destruction under section 63G (i.e. beyond a maximum of six months);

whereas

- a very high proportion of those that have been taken from people who were not suspected of having committed those offences have been retained beyond that time.

In my view this is an unsatisfactory state of affairs, not least in that it may deter people from volunteering DNA samples to the police in connection with the investigation of offences. I intend to look into it more closely and to pursue with the Home Office the possibility that it should issue revised guidance to forces in this connection.

191. When an elimination sample is taken in connection with the investigation of an offence, the consent form which is completed by the donor starts as follows:

> *"I consent to a DNA sample (mouth swab/pulled hair) being taken for forensic analysis. I understand that the resulting profile will only be compared to the crime stain profile(s) from this enquiry and that the samples will be destroyed at the end of this case."*

I am not persuaded that that form adequately alerts donors to the true position as regards the retention of their samples and have suggested that it should be revised so as to do so.[78] This has been accepted by the Home Office and others and I understand that a new and more informative consent form is currently being drafted and will be introduced as soon as possible.

ARRESTEE SAMPLES

GENERALLY

192. The Guidance that has been issued to forces by the Home Office in connection with the CPIA exception states as follows:

> *"It is expected that in the great majority of cases, PACE samples will be destroyed either as soon as a DNA profile has been derived or, if sooner, within six months of the sample being taken.*
>
> *However, there may be some circumstances where a PACE sample is required to be retained as part of casework. Casework must be the expert comparison of DNA evidence by a forensic scientist and not routine DNA matches from the database. If you wish to retain a PACE sample under CPIA for casework, you must ensure that you notify your FSP at the time of submitting the sample for analysis."*

[78] See e.g. CPIA Code D, Annex F, Note F1 which provides that *"It is ... important to make sure ... that [an innocent volunteer's] consent to their ... DNA being used ... is fully informed and voluntary."* This annex is apparently awaiting amendment in the light of PoFA. See also paragraphs 198-199 below.

Given the relatively small number of arrestee samples that are apparently being retained pursuant to the CPIA exception, it seems that forces are acting in accordance with that guidance and that they are giving careful thought to the retention of samples on that basis. It is clear, however, that forces have been taking differing views of the true scope of that exception. A striking feature of the figures that have been made available to me has been that some forces have, it seems, been retaining many more arrestee samples than other forces.

DIP-SAMPLING AND DISCUSSIONS WITH FORCES.

FORCES IN HUMBERSIDE, NORTHUMBRIA AND YORKSHIRE

193. In May of 2014 the figures that I was provided with by the NDU indicated that, of the 819 arrestee samples that were being held pursuant to the CPIA exception by FSPs, 583 (i.e. 71%) were being held by LGC on behalf of 5 forces i.e. Humberside, Northumbria, North Yorkshire, South Yorkshire, and West Yorkshire.

194. In June of 2014 I visited West Yorkshire Police's Scientific Support Unit in Wakefield. That Unit provides scientific support services to the Yorkshire and Humberside forces and LGC is the in-house FSP. I met there with representatives of LGC and those forces, discussed with them their (shared) policies as regards the CPIA exception, and examined the files in 19 cases (including Northumbria cases) in which arrestee samples were being retained in reliance on that exception. Of those cases there were 12 in which retention of the samples seemed to me to be potentially justifiable and 7 in which it was unclear to me why retention had been considered appropriate.

195. Among the points which emerged from that visit and from my other dealings with those 5 forces were:

- that they were uncertain as to the circumstances in which the CPIA exception could properly be relied on in relation to arrestee samples;
- that they were conscious that they were retaining many more samples than most forces and were concerned as to why this was the case: it seemed to them that one possibility was that other forces were failing to retain samples pursuant to the CPIA exception when they ought in fact to be doing so; and
- that they were seeking to develop more appropriate policies in that regard.

It was also apparent, however, that care was already being taken to ensure that the retention of any arrestee sample pursuant to the CPIA exception was kept under regular review and that instructions were given to destroy any such sample if and when it became apparent that that exception no longer applied.

THAMES VALLEY POLICE

196. In August of 2014 I also visited the Forensic Investigation Unit of Thames Valley Police ('TVP') in Kidlington to discuss that force's approach to the retention of DNA samples pursuant to the CPIA exception. Although the figures for 31 March 2014 had indicated that TVP was then retaining 'in force' an unusually large number of samples (i.e. 54) pursuant to that exception, the figures for 30 June 2014 had indicated that that figure had by then fallen to nil. It was explained by TVP that the figure for 31 March had been incorrect in that none of the 54 samples referred to had in fact been held at that date for longer than the retention period allowed for by PoFA.

197. It was again also apparent from that visit:

- that there was uncertainty as to the circumstances in which the CPIA exception could properly be relied on; and
- that work was being undertaken to develop appropriate policies in that regard.

It was also again apparent that the retention of every arrestee sample which was being held in force was being kept under regular review and that care was being taken to ensure that any such sample was destroyed within the retention period allowed for by PoFA unless it was considered appropriate to retain it for a longer period pursuant to the CPIA exception. I was informed that, as at the date of my visit, no arrestee samples were being retained on that basis: this was borne out by a 'dip-sampling' exercise which I then carried out.

DURATION OF RETENTION

198. Under the Code of Practice prepared under section 23 of the CPIA, an investigator *"must retain material obtained in a criminal investigation which may be relevant to the investigation"* and such material "*includes in particular ... material which may satisfy the test for prosecution disclosure"*. All material which should be retained under this Code *"must be retained until a decision is taken whether to institute proceedings against a person for an offence"* and, thereafter:

- if criminal proceedings are instituted, *"at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case"*;
- if the accused is convicted, *"at least until six months from the date of the conviction"* or, if a custodial sentence is imposed, *"at least until the convicted person is released from custody"*; and
- if an appeal against conviction is in progress or an application to the Criminal Cases Review Commission is being considered, at least until that appeal or application is determined.

I understand, however, that although those are the relevant minimum retention periods, all material that is retained pursuant to the Code is in practice likely to be retained for the entirety of the relevant minimum *file* retention period as provided for in Guidance issued by

the National Policing Improvement Agency in 2012. The minimum file retention periods set out in that Guidance are 30 years for *"major and serious crime"*, 7 years for *"volume crime"*, and 3 years for *"simple possession of drugs cases and alcohol/drugs driving offences"*.

199. In my view it would be extremely unfortunate – and very probably unlawful – if that practice were to be applied to DNA samples that are retained pursuant to the CPIA exception. As amended by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014, section 63U of PACE provides (at subsection 5B) that:

> *"A sample that once fell within subsection (5) [i.e. that once fell within the CPIA exception] but no longer does, and so becomes a sample to which section 63R applies, must be destroyed immediately if the time specified for its destruction under that section has already passed*."

I shall of course carry out appropriate checks to establish whether or not samples are in fact destroyed in line with that provision.

CONCLUSION

200. In summary, then:

- I have found no reason to suspect that there has been significant non-compliance with the sample destruction regime provided for by PoFA; but
- I am concerned that the CPIA exception that was later introduced may be being misapplied.

I intend to keep both those matters under careful review.

201. Although forces appear to have tried hard to make use of the CPIA exception in a sensible and restrained manner, it seems clear that there is widespread uncertainty as to the circumstances in which it can properly be relied on. The Home Office should in my view re-visit and expand upon the Guidance which it has issued to forces in connection with that exception.

202. When re-visiting that Guidance the Home Office should not only give thought to the proper application of that exception to arrestee samples but also to its application to elimination samples. It should in addition ensure:

- that a new and more informative consent form is introduced as soon as possible as regards elimination samples; and
- that forces are reminded of their obligation to destroy both arrestee and elimination samples as soon as the CPIA exception ceases to apply to them.

4.2 DNA PROFILES AND FINGERPRINTS

BACKGROUND

203. As regards DNA profiles and fingerprints (and as has been pointed out earlier in this report) the general rule provided for by PoFA is:

- that they may be retained indefinitely if the individual in question has been or is convicted of a recordable offence; but
- that in almost all other circumstances they must be deleted from the national databases at the conclusion of the relevant investigation or proceedings.

There are, however, exceptions to that general rule, particularly as regards:

- its application to those who commit offences when they are under the age of 18 and/or to whom a Penalty Notice for Disorder (a PND) is issued; and
- where someone is arrested for, albeit not convicted of, a 'qualifying offence'.

As has also been pointed out above, it was understandably decided at an early stage that the retention and deletion of DNA profiles and fingerprints on or from the relevant national databases should be generated automatically by the PNC.

204. In his Written Ministerial Statement of 13 December 2012 Lord Taylor of Holbeach CBE said as regards DNA profiles and fingerprints:

> *"DNA profiles, consisting of a string of 20 numbers and two letters to indicate gender, are stored on the National DNA Database (NDNAD). They allow a person to be identified if they leave their DNA at a crime scene but contain none of the person's genetic characteristics. The NDNAD and the Police National Computer (PNC) must both be reprogrammed to allow DNA profiles which may not be retained under the Act to be correctly identified and deleted. Deletion from the NDNAD of existing DNA profiles which do not meet requirements for retention will begin in January 2013 and be completed by September 2013.*
>
> *Fingerprints are stored electronically on the national fingerprint database, IDENT1. IDENT1 and the PNC must both be reprogrammed to allow fingerprints which may not be retained under the Act to be correctly identified and deleted. Deletion from IDENT1 of fingerprints which do not meet requirements for retention will begin in March 2013 and be completed by September 2013. Following deletion of each IDENT1 fingerprint set, police forces will destroy any corresponding hard copies they hold."*

205. In their further Written Ministerial Statement of 24 October 2013 Lord Taylor and James Brokenshire MP said:

> *"The Government have now delivered their commitment to reform the retention of DNA and fingerprint records by removing innocent people from the databases, and adding the guilty.*
>
> *1,766,000 DNA profiles taken from innocent adults and children have been deleted from the national DNA database. 1,672,000 fingerprint records taken from innocent adults and children*

have been deleted from the national fingerprint database. ... 480,000 of the DNA profiles removed as part of this programme were taken from children."

206. Unlike the position as regards DNA samples, the retention regime provided for by PoFA always contemplated the existence of a CPIA exception as regards DNA profiles and fingerprints. In reality, however, no profiles or fingerprints are retained on the national databases in reliance on that exception and it is of relevance only to hard copies that are retained in case files.

HAVE DNA PROFILES AND FINGERPRINTS BEEN APPROPRIATELY DELETED/DESTROYED?

GENERALLY

207. I have found no reason to doubt the accuracy of the pre-commencement profile and fingerprint deletion figures which were given in the Written Ministerial Statement of 24 October 2013 and it is clear that very considerable efforts have been made to programme the PNC so that profiles and prints are retained on the national databases when, and only when, their retention is lawful under the PoFA regime. In reality, however, it was always clear that that would be an impossible task.

208. There are at least 3 reasons for this.

i. The first is that the PNC was not established to perform such a task and that the cost of adapting it to do so would, it seems, have been very considerable indeed. Given the pressures on police and other budgets and the need to prioritise resources, it is unsurprising that it was decided that the sensible course would instead be:

- to settle for a system which, though generally producing appropriate results, would sometimes lead to material being retained when it should in fact have been deleted; but
- to seek to mitigate the adverse effects of that 'compromise' arrangement by (among other things) providing detailed guidance to forces about checking the lawfulness of any matches with profiles or fingerprints on the national databases before acting on them.

Such guidance has indeed been issued to forces by the Home Office.[79]

ii. The second difficulty in the way of implementing the new retention regime simply by the reprogramming of the PNC is that, as is pointed out above,[80] concepts relied on in PoFA, such as *"the conclusion of the investigation of an offence"*, play no part in the operations of the PNC; it has therefore been necessary to make use of similar

[79] Although my Office has to date been notified of only a handful of matches which have been identified as unlawful, it is impossible to know what the true scale of this problem is. I intend to look further into it and into the question of how it has in practice been addressed by the forces concerned.

[80] See paragraph 32 above.

but not identical concepts – such as the NFA-ing of individual arrestees – as the 'drivers' of automatic deletions. As is also pointed out above, this has in turn made it necessary to introduce specific *ad hoc* processes to cater for, among other things, complex continuing investigations.[81]

iii. The third such difficulty is that the accuracy and usefulness of the PNC are dependent upon its being promptly and correctly updated by the forces which make entries on it. Unless the entries on the PNC are accurate and up-to-date, DNA profiles and fingerprints that should have been deleted from the national databases will be retained on them and, just as important, profiles and prints that should have been retained on those databases will be deleted from them.

DELAYS IN UPDATING THE PNC

209. Significant delays in the updating of the PNC have been brought to my attention on a number of occasions and I have been told that they are commonplace. In the main, the delays which have been raised with me have been delays between individuals being notified that No Further Action will be taken against them and the PNC being updated to that effect. Since the making of an NFA entry on the PNC is the usual trigger for the deletion of an individual's DNA profile and fingerprints from the national databases, a delay in making such an entry will sometimes result in the wrongful retention of such material.

210. Delays in updating the PNC may also have the opposite effect. As is pointed out earlier in this report, if a force is minded to make an application to me under section 63G of PACE it has until 14 days after the 'NFA date' to put on the PNC an appropriate 'marker' which will have the effect of precluding the automatic deletion of the relevant arrestee's biometric records. In one case the force in question overlooked that deadline and, as a result, that arrestee's records were deleted and the application had to be withdrawn.

211. I have raised my concerns about delays in updating the PNC with officials at the Home Office, with the NDNAD Strategy Board and with others. I am as yet uncertain as to the true extent of the problem and intend to pursue my investigations into it over the coming months.

OTHER PNC PROBLEMS

212. There are four other matters relating to the programming and operation of the PNC to which I should make specific reference. Three relate to matters which have had the effect of causing DNA profiles and fingerprints to be retained on the national databases when they should in fact have been deleted and the other has had the reverse – but no less serious – effect i.e. that of deleting from those databases biometric data that could and should have been retained on them. I deal first with that 'wrongful deletion' problem.

[81] See paragraphs 67-69 above.

ERRONEOUS DELETIONS

213. This issue first came to my attention in early April 2014 when it became apparent that, in a number of the cases in relation to which the MPS had made applications to me, the biometric material at issue had wrongly been deleted as a result of a PNC programming error. I immediately raised this with the PNC Services Team who produced, at my request, a formal report on this problem which I shared with the NDNAD Strategy Board and with Home Office officials.

214. Although I have been assured that the software issue in question has now been remedied, it has not yet been possible to identify precisely how many records which should have been retained were in fact deleted as a result of it. It is clear, however, that at least 5 individuals' biometric records – which the MPS particularly wanted to be retained – were erroneously deleted, and it seems likely:

- that around a further 25 individuals' records were also erroneously deleted as a result of this problem; and
- that of the records held on 26 April 2014, those of 114 individuals might well have been erroneously deleted if the problem had not been identified and remedied.

Having taken advice as to whether or not they could require the 5 individuals in respect of whom they had made applications for extended retention to provide them with replacement samples, the MPS withdrew those applications.

PROCEEDINGS STAYED

215. A second problem associated with the programming of PNC arose in connection with entries to the effect that proceedings had been 'stayed', particularly in circumstances where an indictment had been replaced and the accused had then been tried and acquitted on a substitute indictment. I became aware of that problem when I was approached by an individual who had, in those circumstances, been unable to obtain confirmation from the police that his biometric records had been deleted from the national databases in line with the requirements of PoFA.

216. On 18 June 2014 I discussed that and other PNC issues at a meeting with, among others, ACC David Pryde, the ACPO lead on PNC matters. At that meeting I was informed that, although on a 'worst case scenario' 15 to 20,000 cases could be affected by this 'stay' problem, the actual number of cases affected was likely to be very much lower. I have no reason to doubt that assessment.

217. It was agreed that steps would be taken:

- to prevent that problem arising after 9 July 2014 by issuing appropriate guidance to forces and by introducing an appropriate technical 'fix' as regards future PNC entries; and

- to devise and introduce by the end of October 2014 a further technical 'fix' which would remedy the past consequences of that problem.

I understand that the necessary technical 'fixes' have been put in place and that this problem has now been resolved save only as regards approximately 300 entries which were made on the PNC before 9 July 2014. I further understand that any retention errors which flow from those entries will be remedied within the next few weeks.

'DISCONTINUED – OTHER' ENTRIES

218. A third problem associated with the programming of PNC became apparent in connection with 'discontinued – other' entries. Such an entry is, it seems, made on the PNC when proceedings in a Magistrates' Court are discontinued before trial (whether or not it is open to the CPS to revive them). At the meeting on 18 June 2014 I was informed that this problem could, as with the 'stay' problem, result in the retention of biometric records when they should in fact be deleted. It was suggested that, on a 'worst case' estimate, the problem could have led to unlawful retention in about 140,000 cases but that the true figure was likely to be very much smaller. Once again I have no reason to doubt that assessment.

219. Various possible ways of addressing this problem were discussed at that meeting and at a later meeting of the PoFA Implementation Board.[82] One difficulty that arose was that of ensuring that any technical 'fix' which was aimed at ensuring that biometric material was not retained unlawfully as a result of this 'discontinued – other' problem, should so far as possible avoid running the risk of deleting material which could and should in fact be retained (e.g. in circumstances where the 'discontinued' proceedings are in fact revived).

220. In the event it was decided that the most appropriate (albeit imperfect) course would be to devise a programme whereby biometric records would be retained for six months after the making of such an entry but would thereafter be deleted unless they were subject to retention on some other grounds. This proposed approach seemed to me to be a sensible one and it was my understanding that the necessary re-programming work – which would be both retrospective and prospective in its effect – would be completed by the end of 2014 at the latest. To my concern, however, I have recently been informed that this is most unlikely to be the case and that even a start-date for that work has yet to be fixed. I shall, of course, continue to pursue the matter.

WANTED/MISSING MARKERS

221. A further PNC-related problem arises out of the fact that any 'Wanted/Missing' marker on PNC will prevent the deletion of biometric records even if those records cannot lawfully be retained. I became aware of a number of cases where this had happened – an example

[82] The 'PoFA Implementation Board', meetings of which I attend as an observer, was set up to oversee the implementation of PoFA.

being where a 'wanted/missing' marker was put on the PNC in connection with a civil 'harassment' order – and took steps to establish just how big this problem really was.[83] Although differing views have been expressed in that regard, it seems generally to be accepted that there is a significant erroneous retention problem associated with Wanted/Missing markers and there seem to me to be reasonable grounds to believe that in April of 2014 the biometric records of approximately 4,300 individuals were being wrongly retained as a result of that problem.

222. I understand that it is unlikely that this 'Wanted/Missing' problem can wholly be resolved and that it is probable that it will continue to prevent the deletion of at least some biometric records that cannot lawfully be retained. Equally however, I understand that work is planned for next year which is likely to reduce by over 95% the number of records that are affected by the problem.

COPIES

223. New section 63Q of PACE provides that:

> *"(1) If fingerprints are required by section 63D to be destroyed, any copies of the fingerprints held by the police must also be destroyed.*
>
> *(2) If a DNA profile is required by that section to be destroyed, no copy may be retained by the police except in a form which does not include information which identifies the person to whom the DNA profile relates."*

224. As regards copies of DNA profiles, I have no reason to suspect significant non-compliance with that provision. I note in particular:

- that it is, it seems, only in very unusual circumstances that the police are or have been supplied with electronic or hard copies of DNA profiles rather than with 'match reports' in relation to them;
- that forces do not maintain local databases of DNA profiles and that it would be very difficult indeed for them to procure that an unlawfully held copy of a DNA profile was loaded to, or searched against, the national database; and
- that it is clear that extensive work has been done to ensure the appropriate deletion or 'de-linking' of electronic copies of DNA profiles from the IT systems of FSPs.[84]

I also note that it is intended that the 'PoFA compliance checks' that are to be carried out by UKAS in relation to FSPs[85] will include checks on their handling of such copies.

225. As regards copies of fingerprints, however, the position is more complicated, not least because:

[83] I am very grateful to David Low, Specialist PNC Policy Advisor for the Metropolitan Police, for the assistance he has given me in relation to this and other matters.

[84] De-linking breaks the link between a DNA profile and its associated demographic information.

[85] See paragraph 184 above.

- it has until recently been normal practice for the police to make and retain hard copies of arrestees' fingerprints; and
- in addition to the fingerprint data that is contained on IDENT1, police forces commonly maintain and use their own searchable databases of fingerprints that are thought likely to be of use in their local areas.

As to the second of those factors it must at least be possible that, notwithstanding the advice that has been issued to forces, electronic copies of fingerprints that should have been deleted from local databases have in fact been retained on them. It has recently become apparent that such copies have been retained on national fingerprint training databases and I intend to do some dip-sampling work on local police databases over the next year or so.[86] Although little of substance is likely to turn upon the failure to update the training databases, the appropriate 'cleansing' of local databases is, of course, almost as important as the appropriate 'cleansing' of IDENT1.

226. As to the first of the factors referred to above – the problems that arise as regards hard copies of fingerprints – the logistical challenges were always likely to be considerable. Those challenges were acknowledged when PoFA was brought into effect in that forces were allowed an additional three month period (i.e. until 31 January 2014) to comply with their destruction obligations in that connection.[87] In the event – and at least as regards the National Archive of hard copy fingerprints – those obligations were not discharged by even that delayed implementation date.

227. The National Archive is held by the MPS and contains several million hard copy sets of fingerprints dating back to before 1908. It seems likely that many of those hard copy sets – up to around 154,000 'unreconciled' records[88] – cannot lawfully be retained under the new PoFA regime. It has also been suggested, however, both that hard copy fingerprints in that collection can sometimes be of real practical value in the context of an investigation and that it would be impossible to 'cleanse' that collection in line with the requirements of PoFA otherwise than by way of an extremely time-consuming and expensive manual 'weeding' exercise.

228. In those circumstances it was proposed that, rather than embarking on such an exercise, safeguards should be introduced whereby, when forces seek access to records in that collection:
    - checks will be made as to whether or not the copy fingerprints at issue are in fact copies which fall for destruction under (new) section 63Q(1) of PACE;

    and, if that proves to be case,

[86] I understand that it is hoped that the training databases will be fully updated within the next 2 years.

[87] See http://www.legislation.gov.uk/uksi/2013/1814/contents/made

[88] 'Unreconciled' hard copy prints do not have a corresponding PNC record or digital record on IDENT1.

- those records will not be made available to the requesting force but will instead be destroyed forthwith.

229. The intended (and in my view likely) effect of those proposed safeguards would be to ensure that:

(i) hard copy fingerprints which fell within the ambit of section 63Q(1) would ultimately be destroyed; and

(ii) that in the meantime the police will be unable make any use of them.

This proposed course was endorsed by the Information Commissioner's Office and a decision has been taken by the Home Office to adopt it. I will, of course, take steps to monitor its operation and effectiveness. I also intend – as with electronic copies of fingerprints on local police databases – to do some dip-sampling work on local police collections of hard copy fingerprints.

THE CPIA EXCEPTION ETC.

230. As is mentioned above, the retention regime provided for by PoFA always contemplated the existence of a CPIA exception as regards DNA profiles and fingerprints and that exception may be of relevance to hard copies that are retained in case files.[89] Three points are worth noting in that regard.

i. It is, it seems, only rarely that hard copies of DNA profiles – rather than 'match reports' – will be placed in case files. Where they are, moreover, little (if any) practical use can be made of them by the police and, in particular, they cannot be used to re-load profiles to the NDNAD. By contrast – and whether or not the CPIA exception applies – it is apparently quite common for hard copy fingerprints to be kept in case files and it would be possible for a force to use those copies to search against IDENT1 and/or its local fingerprint database.

ii. Unlike the position as regards DNA samples that are retained pursuant to the CPIA exception, there are no express legislative restrictions as to the use that can be made of DNA profiles and fingerprints that are retained pursuant to that exception or as to the period for which they can be retained. Even so, it seems clear that they cannot lawfully be retained by the police after they cease to fall within that exception if the time specified in PACE for their destruction has already passed. By section 63T(2) of PACE, moreover, material which should have been destroyed must not after that time "*be used in evidence against the person to whom the material relates, or for the purposes of the investigation of any offence*."

iii. I understand that as a general rule (and as is pointed out above) all material that is placed in a case file – whether pursuant to the CPIA exception or otherwise – is retained for the entirety of the relevant minimum file retention period (i.e. 3, 7 or 30

[89] See paragraph 206.

years).[90] This seems to be the position not only as regards hard copies of DNA profiles and fingerprints which have been taken from arrestees but also as regards hard copies of profiles and prints which have been given voluntarily (e.g. for 'elimination' purposes) and which can lawfully be retained only until they have *"fulfilled the purpose for which [they were] taken or derived."*[91] Against that background it seems likely that some hard copies of DNA profiles – and, perhaps more importantly, that substantial numbers of hard copies of fingerprints – are being unlawfully retained in case files. Equally, however, it seems likely that the cost of 'weeding' all those case files so as to remove any such copies would be considerable.

231. It may well be that it would be sensible to review – and shorten – the existing retention periods for case files and I intend to raise that possibility with other interested parties. Since, moreover, the consent forms which are currently completed by those who volunteer fingerprints fail to alert them to the true position as regards the retention of their prints, it would also seem sensible for those forms (like the consent forms in respect of DNA samples) to be revised so as to do so.

CONCLUSION

232. I have no reason to doubt that the overwhelming bulk of the DNA profiles and fingerprints that should have been deleted from the national databases under the new PoFA regime have indeed been deleted. I likewise I have no reason to doubt that the overwhelming bulk of the profiles and prints that should be being retained on those databases are indeed being retained.

233. Given the limitations of the PNC it was always inevitable that some 'wrongful' retentions and deletions would occur and this has proved to be the case. Save only as regards the 'Discontinued – Other' problem which is referred to at paragraphs 218-220 above, I am satisfied that real efforts have been made to minimise those wrongful retentions and deletions and, so far as is possible, to address their causes when they have been identified. Despite those efforts, however, it seems likely:

- that at least a small number (c. 30) DNA profiles and fingerprints which should have been retained on the national databases have in fact been deleted; and
- that at least some thousands of profiles and prints which should have been deleted have in fact been retained.

I shall of course continue to monitor any PNC-related issues and to press for their speedy resolution.

[90] See paragraph 198 above.

[91] See Section 63N(2) of PACE.

234. I am uncertain as to the position as regards local police (fingerprint) databases but have as yet no reason to believe that it differs substantially from that as regards IDENT1 or that those databases are other than broadly, albeit not wholly, compliant with the PoFA regime.

235. It also seems likely that substantial numbers of hard copies of fingerprints are being retained otherwise than in compliance with the PoFA regime, particularly in the 'National Archive' and in case files. I have, however, no reason to suspect that improper use is being made of those hard copies.

236. I intend to keep all these matters under careful review.

4.3 EARLY DELETION AND THE EXCEPTIONAL CASE PROCEDURE

237. Section 63AB of PACE (as introduced by section 24 of PoFA) provides as follows.

> *"(2) The National DNA Database Strategy Board must issue guidance about the destruction of DNA profiles which are, or may be retained under this part of the Act.*
>
> *(3) A chief officer of a police force in England and Wales must act in accordance with guidance issued under subsection (2)."*

238. In January of 2014 the Strategy Board issued Guidance under section 63AB(2) in which it established an 'Early Deletion Process' under which individuals may apply to Chief Constables to have their DNA profiles and/or fingerprints deleted from the national databases before the expiry of the maximum retention periods allowed for under the PoFA regime.[92] Under the Early Deletion Process:

- an application for early deletion will be considered only if it is made by an applicant without previous convictions who has been given a PND or who has been charged with, but not convicted of, a qualifying offence; and
- such an application will be successful only if the applicant both satisfies those criteria and has been eliminated as a suspect for the offence for which he or she was arrested.[93]

[92] See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273744/DNA_early_deletion_process_v1.pdf

There is currently a separate 'Exceptional Case Procedure' under which individuals may apply to Chief Constables to have their PNC records deleted. A successful application under that procedure will also result in the deletion of that individual's DNA profile and fingerprints. It is intended that these two processes should soon be consolidated and that the Early Deletion Process should be extended so as to apply to applications of both sorts.

[93] Although at Paragraph 12 viii. of the Early Deletion Guidance it is suggested that a Chief Officer may order early deletion if he or she *"determines that there is a wider public interest to do so"*, at Paragraph 9 iv. of the same Guidance, and in the first sentence of Paragraph 12, it is made clear that elimination as a suspect is a necessary precondition of (discretionary) early deletion.

In my view (and as I made clear during the public consultation which took place before the Strategy Board Guidance was issued)[94] these conditions are much too restrictive and early deletion should be available in a much wider range of situations.

239. In the Early Deletion Guidance it is observed (at Paragraph 3) that the power of retention under the legislation in force in the period leading up to the enactment of PoFA was permissive and not mandatory. The powers of retention which are provided for in PoFA are likewise permissive rather than mandatory. The proposition that the relevant legislation allowed – but did not require – the police to retain indefinitely arrestees' DNA samples, DNA profiles and fingerprints was central to the reasoning in the majority judgments in *R (GC) v The Commissioner etc,*[95] a case in which the Supreme Court declared unlawful the ACPO Guidelines in respect of the 'Exceptional Case Procedure'.[96]

240. The maximum retention period which is provided for in respect of an individual without previous convictions who has been given a PND is 2 years from the taking of the relevant DNA sample or fingerprints. The maximum retention period which is provided for in respect of an individual without previous convictions who has been charged with, but not convicted of, a qualifying offence is (absent a successful application to a District Judge for an extension) 3 years from the taking of the relevant sample or fingerprints. By allowing for early deletion only in the very restricted circumstances which are summarised above, the Strategy Board has in effect ruled:

    (i) that every other maximum retention period which is provided for by PoFA should be treated not only as a maximum retention period but also as a minimum retention period; and

    (ii) that early deletion should be available only in circumstances where an individual's DNA profile or fingerprints may be retained for a relatively short period and not where they may be retained for a much longer period or even indefinitely.

Furthermore, notwithstanding the genesis of the 'biometric' provisions of PoFA no reference is made in the Guidance to issues of privacy or proportionality and no provision is made for Chief Officers to carry out of any kind of balancing exercise as regards the retention of the material at issue. Decisions on early deletion are, it seems, to turn primarily (and perhaps solely) on the existence or otherwise of substantial evidence that the individual in question is no longer a suspect for the offence for which they were arrested. In the absence of such evidence those decisions are, it seems, to be made entirely without reference to factors such as the age, nature and seriousness of the alleged offence at issue; the age and subsequent history of the individual applicant; or the cogency of any reasons for believing that the public interest will be served by continued retention.

---

[94] https://www.gov.uk/government/publications/biometrics-commissioners-response-to-draft-guidance-on-early-deletion

[95] [2011] UKSC 21, especially at Paragraphs 24, 25, 27, 30, 33 and 35.

[96] See footnote 92 above.

241. It is not difficult to conceive of circumstances which would fall outwith the ambit of the Early Deletion Process but in which the continued retention of an individual's DNA profile or fingerprints might well be considered unnecessary and disproportionate. Such circumstances might well arise, for example, where that continued – and, indeed, indefinite – retention could be 'justified' only by reference to the fact that many years previously the individual in question had accepted a caution for a minor offence.

242. Against that background there must, in my view, be scope for real doubt as to whether an Early Deletion Process which is available only in the very restricted circumstances which have been approved by the Strategy Board takes proper account of the principles laid down in *S and Marper v UK*[97] or adequately reflects the spirit or policy underlying the 'biometric' provisions of PoFA.[98] There must likewise be scope for doubt as to whether a 'blanket and indiscriminate' refusal to consider applications for early deletion from, for example, any individual whose DNA profile or fingerprints are subject to indefinite retention (e.g. any adult who has been convicted of, or cautioned for, a recordable offence) would be consistent with a Chief Officer's duty as a Data Controller under the Data Protection Act 1998 to ensure that the retention of sensitive data is at all times proportionate and not excessive.[99]

243. In my view an Early Deletion Process which was significantly less restrictive than that which is provided for in the current Guidance would allow for the striking of a more proportionate balance between the public interest in the prevention and detection of crime and the individual's right to privacy. Such a Process would, moreover, not only allow for more appropriate decisions in a much wider range of individual cases but might also be more likely to command broad public support and thus to assist in maintaining public confidence in those who are authorised to take and retain DNA and fingerprints.[100]

244. I recognise that there might well be concerns that a less restrictive Early Deletion Process than that which is currently in operation might have considerable financial and other resource implications for police forces. Such a Process would not, however, have to be one under which Chief Officers would inevitably be required to make complex individual

[97] (2008) 48 ECHR 1169

[98] It seems likely that further guidance as regards at least the first of those points will be given when the decision of the Supreme Court is handed down in *Gaughran (AP) (Appellant) v The Chief Constable of the Police Service of Northern Ireland (Respondent) (Northern Ireland)* UKSC 2013/0090

[99] See Paragraph 8 of the Guidance and DPA 1998, Schedule 1 Part 1 (3) and (5). See also Schedule 2, at 6(1).

[100] I understand that between January and October of 2014 some 76 applications were made under the Early Deletion Process but that none required a decision to be made as either the applicants were not eligible for early deletion or the biometric records at issue had been – or were just about to be – deleted automatically. Given, however, the overlap between the Early Deletion Process and the Exceptional Case Procedure (as to which see Footnote 92 above) these figures may well be misleading. It seems that during the same period some 2000 applications were made under that Exceptional Case Procedure and that some 367 of those applications were successful (and therefore resulted in the deletion of any DNA profiles and fingerprints that were held from those applicants).

judgments in huge numbers of cases. In that connection – and quite apart from the fact that a specific application would continue to be necessary before the Early Deletion Process was triggered – 'brightline' rules[101] could be introduced which, for example, excluded applications within (say) 3 years of a conviction or caution or where (say) the offence at issue is a 'qualifying' offence as defined at section 65A(2) of PACE.

[101] cf e.g. *R (on the application of RMC and FJ) v MPC* [2012] EWHC 1681 (Admin) at Paragraphs 51 and 54.

5. THE USE TO WHICH BIOMETRIC MATERIAL IS BEING PUT

5.1 GENERALLY

245. By section 20(6)(a) of PoFA I have the function of keeping under review not only the *retention* of DNA samples, DNA profiles and fingerprints (and of copies thereof) but also the *use* of such material and copies *"in accordance with sections 63A and 63D to 63T of [PACE]"*.

246. Section 63T of PACE (which was introduced by section 16 of PoFA) provides as follows.

> *"**63T Use of retained material***
>
> *(1) Any material to which section 63D, 63R or 63S applies must not be used other than—*
>
> *(a) in the interests of national security,*
>
> *(b) for the purposes of a terrorist investigation,*
>
> *(c) for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution, or*
>
> *(d) for purposes related to the identification of a deceased person or of the person to whom the material relates.*
>
> *(2) Material which is required by section 63D, 63R or 63S to be destroyed must not at any time after it is required to be destroyed be used—*
>
> *(a) in evidence against the person to whom the material relates, or*
>
> *(b) for the purposes of the investigation of any offence.*
>
> *(3) In this section—*
>
> *(a) the reference to using material includes a reference to allowing any check to be made against it and to disclosing it to any person,*
>
> *(b) the reference to crime includes a reference to any conduct which—*
>
> *(i) constitutes one or more criminal offences (whether under the law of England and Wales or of any country or territory outside England and Wales), or*
>
> *(ii) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences, and*
>
> *(c) the references to an investigation and to a prosecution include references, respectively, to any investigation outside England and Wales of any crime or suspected crime and to a prosecution brought in respect of any crime in a country or territory outside England and Wales."*

I have seen nothing to suggest that DNA samples, DNA profiles or fingerprints – or copies of such profiles or prints – are being used otherwise than in accordance with with section 63T.

247. Two matters relating to the use to which biometric material is put appear to me to merit particular mention. They are:

- speculative searches of DNA profiles and fingerprints; and
- the international sharing of such profiles and prints.

I deal with those matters in that order.

5.2 SPECULATIVE SEARCHES

BACKGROUND

248. The basic rules governing the destruction and deletion of DNA profiles and fingerprints are set out at section 63D of PACE (which was introduced by section 1 of PoFA). Section 63D(5) provides:

> *"(5) Nothing in this section prevents a speculat ive search, in relation to section 63D material, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable*."

A speculative search allows the relevant DNA profile and fingerprints to be checked against existing holdings on the national databases – and, perhaps most importantly, against existing holdings of crime scene DNA profiles and unidentified 'fingermarks' – to determine if there is a match.

249. The right to make such a search is of particular importance in circumstances where an arrestee without previous convictions is quickly NFA'd and his or her biometric records therefore fall to be deleted. The problems which have arisen in this connection relate to the difficulty of ensuring both:

- that those biometric records are not retained on the databases for an excessive period, particularly in circumstances where they are constantly being searched against other records;[102] and
- that the right to conduct a speculative search is a genuinely valuable one and, in particular, that sufficient time is allowed for the results of such a search to be properly checked and, if appropriate, acted upon.

As time has gone on, concerns about that first point have diminished whereas, at least for some, concerns about the second have grown.

250. When considering those issues it is important to appreciate that there are significant differences between the processes involved in the conduct of a speculative search of an individual's DNA profile and those involved in the conduct of a speculative search of his or her fingerprints. It is also important to understand how profiles and fingerprints come to be deleted from the national databases once the time for a speculative search has expired.

[102] It will be noted that section 63D(5) of PACE refers to "a speculative search" rather than to "speculative searches".

DNA PROFILES

251. Although a DNA sample will be taken on arrest, it will take some time, usually between 3 and 14 days, for a profile to be generated from that sample. Once a profile is generated it will be loaded to the NDNAD and automatically searched against all the arrestee and crime scene profiles on that database. It will immediately be apparent whether or not there is a 'match'.

FINGERPRINTS

252. Fingerprints are also taken on arrest, usually by way of a LiveScan machine which communicates directly with IDENT1.[103] Those 'ten-print' sets can immediately be searched against one or more 'caches' of prints on that database, including the cache containing 'unidentified crime scene marks'.[104] Particularly as regards unidentified marks, however, such a search will not simply produce a 'match/no match' result: it will instead produce a number of 'responses' (i.e. possible matches) for consideration by the relevant fingerprint bureau. A response will only be treated as an 'identification' (i.e. a match) when a fingerprint expert has checked the response against the unidentified mark and, having confirmed it as a match, made an appropriate entry on the IDENT1 system. An identification must then be further verified by two independent experts. Either before or after that further verification, an appropriate 'marker' may be placed on the PNC in order to prevent the deletion of the relevant ten-print set.

253. Quite apart for the need for possible matches to be verified by fingerprint experts, a possible cause of delay as regards the identification of a match between an arrestee's fingerprints and an unidentified mark on IDENT1 arises out of the fact that, although a 'ten-print to ten-print' search will always be launched automatically to confirm identity when prints are taken on a LiveScan machine, forces can choose whether or not to launch at the same time a 'ten-print to crime scene mark' search. Perhaps surprisingly – and apparently with a view to regulating the workloads facing their fingerprint bureaux – some forces choose not always to launch that second search immediately but instead opt to do so at a later stage.

DELETIONS

254. The deletion of an arrestee's DNA profile and fingerprints is driven by the PNC and the two records are deleted simultaneously. Unlike the National DNA Database, IDENT1 cannot automatically notify the PNC that a speculative search has or has not been completed. Therefore, when the NDNAD notifies the PNC that there is no match against a searched DNA

[103] Where LiveScan is not available, traditional wet prints are taken with paper and ink. These are then scanned to IDENT1.

[104] I understand that, strictly speaking, IDENT1 should be seen as a collection of linked databases rather than as a single database with separate caches. In this present context, however, the latter terminology seems less likely to give rise to confusion.

profile, this triggers the PNC to delete both the DNA profile and the associated fingerprints on IDENT1 unless a marker has been placed on the PNC following a verified fingerprint match.

THE TRANSITIONAL ARRANGEMENTS

255. When PoFA commenced on 31 October 2013 the development of an automated speculative search process had yet to be completed and transitional arrangements were therefore put in place. During the transitional period – which lasted from 31 October 2013 to 15 June 2014 – DNA profiles and fingerprints were retained on the national databases for a minimum of 63 days from an NFA date. If by the end of that period no 'match' had been declared and there was no other basis upon which they could lawfully be retained, they were deleted from those databases.

256. In view of the length of time for which, under these transitional arrangements, profiles and fingerprints were retained on the databases – and the fact that throughout that period they were or could be repeatedly searched against existing and new arrestee and crime scene profiles and marks – there were understandable concerns as to whether those arrangements complied with the letter and spirit of the new regime. It appears to have been concluded, however, that no reasonable alternative arrangements were available at an acceptable cost.

THE AUTOMATED SPECULATIVE SEARCH PROCESS

257. A new speculative search process became operational on 16 June 2014. Under the new process, biometric material relating to arrests for qualifying offences is treated differently from material relating to arrests for non-qualifying offences. I deal first with what happens if no match is declared against either of the databases and then with what happens if such a match is declared.

QUALIFYING OFFENCES

258. Under the new process, the DNA profile and fingerprint records of an individual without previous convictions who has been NFA'd for a qualifying offence are retained on the national databases for 14 days following the NFA disposal. This allows time for speculative searches to be carried out against both the National DNA Database and IDENT1 before those records become subject to automatic deletion.

THE DNA PROFILE

259. Once loaded and searched against the National DNA Database, the DNA profile is rendered unsearchable. If there is no match against the NDNAD, the 14-day period referred to above should (and was apparently intended to) allow time for a 'UZ' marker to be placed on the PNC if the relevant force wishes to make an application to me under section 63G for consent

to retain the biometric records for an extended period. If such an application is made and the relevant marker is placed on the PNC, the DNA profile will become searchable again for the duration of the section 63G application process. If no UZ (or other) marker is added to the PNC, the DNA profile and fingerprints will be automatically deleted 14 days after the NFA date.[105]

THE FINGERPRINTS

260. The arrestee's fingerprints will remain on IDENT1 for 14 days following the NFA disposal and can be searched against crime scene marks during that period. There is no facility on IDENT1 whereby fingerprints which have been loaded to that database can be rendered unsearchable. As a result, each time a new crime scene mark or ten-print set is loaded to IDENT1 and searched against the 'Unified Collection', the arrestee's fingerprints will be searched. This is a significant difference between the operation of the speculative search process on the NDNAD and its operation on IDENT1.

NON-QUALIFYING OFFENCES

261. For biometric records relating to an arrest for a *non*-qualifying offence, there is no minimum 14-day period during which speculative searches can be carried out. If there is no match resulting from a search against the NDNAD then, as soon as that search is completed, the NDNAD sends a message to the PNC which will (unless the PNC has already been notified of a fingerprint match) cause both the DNA and fingerprint records to be deleted. The DNA profile will immediately be rendered non-searchable and the deletion will take place overnight.

262. In those circumstances the fingerprint records will be deleted at the same time as the DNA profile, regardless of whether they have been searched or not. As with qualifying offences, the fingerprint records will remain searchable – and will continue to be searched against – for as long as they are held on the IDENT1 database.

[105] If, unusually, the profile is not loaded to the NDNAD until after that 14-day period, it will be loaded, searched and (if there is no match) immediately deleted.

DATABASE MATCHES

263. If an arrestee's DNA profile is speculatively searched and there *is* a match against a crime scene or subject profile held on the NDNAD, the arrestee profile remains on the database in a non-searchable form. A match report is produced by the NDNAD and sent to the relevant police force. The police force has one month to decide whether they wish to investigate the match. If they do, the force must place an 'AI' (or 'under investigation') marker on the PNC which will prevent the profile being deleted at the end of that period and will cause it to become searchable once more. Thereafter, if no further updates are added to the record, the PNC will issue a reminder notice one month after the date on which the 'under investigation' marker was added. This reminds the force that if no further update is added to the PNC, the biometric records will be deleted after one month.

264. A similar process applies if an 'under investigation' marker is placed on the PNC following a confirmed fingerprint match (i.e. monthly reminders will be issued and automatic deletion will take place unless appropriate updates are added to the PNC).

ISSUES ARISING

RETENTION PERIODS

265. Under the Automated Speculative Search Process the periods for which DNA profiles and fingerprints are being retained for the purpose of a speculative search are much shorter than was previously the case. Moreover, the fact that the former are largely being retained in a non-searchable form further reduces the extent to which that retention infringes the privacy of the individuals concerned.

266. It is unfortunate that it is currently impossible to retain fingerprints in a non-searchable form in the Unified Collection cache on IDENT1[106] and the introduction of such a facility would bring the speculative search process more fully into line with both the letter and the spirit of the new regime. It would certainly seem desirable for such a facility to be made available when, as is intended,[107] the IDENT1 service is replaced.

THE VALUE OF A SPECULATIVE SEARCH

TIME PRESSURES AS REGARDS FINGERPRINTS

267. As mentioned above, when the National DNA Database notifies the PNC that there is no match against a speculatively searched DNA profile, this triggers the PNC to delete both the DNA profile and the associated fingerprints unless an 'under investigation' marker has been placed on the PNC following a confirmed fingerprint match. When the process was being

[106] See footnote 102 and paragraph 260 above. I understand that, by contrast, fingerprints held on the CT Fingerprint Database can be rendered unsearchable.

[107] See paragraph 320 below.

set up, it was expected that the speculative search process as regards fingerprints would almost always be completed before the speculative search as regards DNA profiles. In practice, however, DNA profiles are now being loaded and searched much more quickly than was anticipated.

268. It has been suggested by the MPS that this has caused, or may cause, difficulty in the context of arrests for non-qualifying offences in that a DNA profile may be loaded and searched – and a deletion message may be sent by the NDNAD to the PNC – before the relevant fingerprint bureau has had sufficient time to complete the fingerprints search, to confirm a match, and to place an 'under investigation' marker on the PNC.[108] As a result (so it is suggested) fingerprints which should be retained because they match crime scene marks may in fact be deleted and the public may in consequence be put at unnecessary risk. The MPS has argued that, in order to address that problem, the minimum 14-day retention period which applies as regards qualifying offences should be extended to cover all offences.

269. I have had numerous meetings about this issue with Home Office officials and with representatives of the MPS and I accept:

- that it is important that the carrying out of speculative searches does not lead to the unnecessarily lengthy retention of DNA profiles and fingerprints which should in fact be deleted; and
- that the true scale of the problem identified by the MPS is as yet unclear and that, as Home Office officials have suggested, it may be that it can adequately be addressed by the appropriate prioritisation of the work of forces' fingerprint bureaux.[109]

Equally, however, I also accept:

- that it is important that fingerprints which match crime scene marks are not deleted before the police have had a reasonable opportunity to investigate that match; and
- that the amendment to the existing process which has been proposed by the MPS (i.e. the extension to non-qualifying offences of the minimum 14-day retention period which applies as regards qualifying offences) would have only a relatively limited impact on the privacy of the individuals involved.

270. Discussions about this issue are ongoing and I shall of course continue to keep it under close review. I note that advances in forensic technology – and, in particular, that any future introduction of 'Rapid DNA' profiling – may well add to the difficulties which forces face

[108] A similar problem may also arise if, as sometimes happens, it proves impossible to derive a profile from a DNA sample or if no such sample is taken. If no DNA profile is loaded to the NDNAD in a case where an arrestee without previous convictions is NFA'd for a non-qualifying offence, his or her fingerprints will be deleted from IDENT1 within 24 hours – and possibly within a matter of minutes – unless an 'under investigation' marker has in the meantime been placed on the PNC.

[109] No other force has raised this matter with me and one has expressly informed me that, so far as it is aware, it has to date lost no material due to the 'primacy' of the DNA search process.

when seeking to ensure that fingerprints are not deleted from the national database before crime scene matches are verified and investigated.

SPEED OF SEARCHING

271. It would seem obviously desirable that a 'ten print to crime scene mark' search of an arrestee's fingerprints should be launched – and that the results should if possible be checked – while the arrestee is still in custody. It is clear, however, that although it is open to forces to launch such a search at that time, this is (apparently for resourcing reasons) by no means universal practice. Given the public safety implications of this matter, it is one which I intend to look into more carefully.

THE NEED FOR AN ARREST

272. An issue has arisen as to whether, if a speculative search results in a confirmed match, the police can lawfully retain the biometric material at issue whilst they are investigating that match without first arresting the relevant individual. Currently, Home Office guidance indicates that police forces may retain that material (by adding, and subsequent updating, an 'under investigation' marker on the relevant PNC record) for as long as they choose while they are investigating the match and without having to arrest that person. This seems to be at odds with the relevant provisions of PACE[110] which, on the face of things, appear to indicate that the material cannot be used in the investigation of an offence absent an arrest. It may therefore be that, unless the legislation is amended, changes will be required to relevant police practice and Home Office guidance. Although I have raised this with the Home Office, I have yet to learn how it views the matter: I shall of course keep it under review.

5.3 INTERNATIONAL DATA SHARING

GENERALLY

273. One aspect of my oversight role as regards the use to which to which biometric material is being put is that of overseeing the sharing of such material internationally. The Home Office's *International DNA Searching Policy for the United Kingdom* states that:

> *"The role of the Biometric Commissioner, once appointed, will be to dip sample cases in which DNA subject material has been transferred out of the UK to make sure that it has been undertaken appropriately."*

Although there appears to be no similar document which formalises my role as regards the international exchange of fingerprints, I have adopted the same approach to fingerprints as to DNA samples and profiles.

[110] See sections 63D(3), 63E, 63P and 63T(2).

274. In the exercise of my functions in this connection I have visited the offices of the National Crime Agency (the NCA) and of the Association of Chief Police Officers Criminal Records Office (ACRO). I have also met on various other occasions with representatives of the NCA and of ACRO and with relevant Home Office officials.

THE ROLES OF THE NCB AND ACRO

275. The National Crime Bureau (the NCB) within the NCA has a coordination and liaison function as regards the exchange of biometric material between the UK and foreign/international law enforcement agencies. It deals with international fugitives and European Arrest Warrants and the case management of international enquiries. Save only for matters relating to counter-terrorism, all requests for the international exchange of DNA profiles are channelled through the NCB. The NCB also deals with the international exchange of fingerprints for intelligence purposes.

276. ACRO oversees the international exchange of criminal records and the loading to the PNC of the foreign convictions of:

- UK nationals who have been convicted of recordable offences abroad; and
- foreign nationals who are resident in the UK and have been convicted of qualifying offences abroad.[111]

ACRO also has responsibility for the international exchange of the fingerprints of convicted people.

EXCHANGE OF FINGERPRINTS IN THE CONTEXT OF CONVICTION INFORMATION

EXCHANGES WITH EU MEMBER STATES

277. ACRO exchanges criminal conviction data with the other 27 EU member states under Framework Decision 2009/315/JHA. Exchanges take place pursuant to 'Requests' or 'Notifications'.

REQUESTS

278. A 'Request Out' is made when a national of another member state is subject to criminal proceedings in the UK. The request is sent to the country of nationality and seeks information about the subject's convictions (if any) in that state. Sometimes that request will be accompanied by the subject's fingerprints. On average, approximately 55 sets of fingerprints relating to (non-UK) EU nationals are sent each month to EU member states in connection with Requests Out.

279. A 'Request In' may be received by ACRO from another EU member state when a UK national is subject to criminal proceedings in that state. The request seeks information about the

[111] Problems which have arisen as regards those matters are addressed at paragraphs 91-99 above.

subject's convictions (if any) in the UK and will sometimes (albeit very rarely) be accompanied by the subject's fingerprints. These fingerprints are used to carry out a 'hit/no hit' search on IDENT1. Between May 2012 and February 2014 only one set of fingerprints was received from another EU member state in connection with a Request In.

280. UK nationals' fingerprints are not sent from the UK to other EU member states in the context of Requests.

NOTIFICATIONS

281. A 'Notification' of conviction information is *sent out* by ACRO when a national of another member state is convicted in the UK. That Notification is sent to the country of nationality and may be accompanied by the subject's fingerprints. If so, those fingerprints will also be sent to Interpol. On average, approximately 800 sets of fingerprints relating to convicted (non-UK) EU nationals are sent each month to EU member states and Interpol in connection with Notifications.

282. UK nationals' fingerprints are not sent from the UK to other EU member states in the context of Notifications.

283. Notifications are *received* by ACRO from other member states whenever a UK national is convicted in another EU member state. Fingerprints are rarely received in that context: only around twice per month. The relevant conviction information is loaded to the PNC and, when fingerprints are received, they are loaded to IDENT1.

EXCHANGES WITH NON-EU COUNTRIES

284. ACRO also exchanges conviction information and fingerprints with non-EU countries on behalf of the NCA and the Home Office. Those exchanges again take place pursuant to Requests and Notifications and may again involve the exchange of fingerprints. On average:

- approximately 550 sets of fingerprints relating to foreign nationals are sent each month to non-EU countries in connection with Requests Out;
- approximately 100 sets of fingerprints are received each month from non-EU countries in connection with Requests In;
- approximately 300 sets of fingerprints relating to non-UK nationals are sent each month to non-EU countries and Interpol in connection with Notifications; and
- it is very rare for fingerprints to be received from non-EU countries in connection with Notifications.[112]

UK nationals' fingerprints are not sent from the UK to non-UK countries.

[112] I understand that precise figures are not available. I also understand that, as with Notifications which are received from EU member states, the relevant conviction information is loaded to the PNC and, when fingerprints are received, they are loaded to IDENT1.

EXCHANGE OF DNA AND FINGERPRINTS FOR INTELLIGENCE PURPOSES

285. The international exchange of DNA and fingerprints for intelligence purposes is co-ordinated by the NCB; it houses the UK's 'Interpol hub'.

DNA SAMPLES

286. DNA samples are very rarely exchanged. The NCB is aware of only one case where it has been agreed that a UK DNA sample should be released to a foreign country. In that case the sample was requested in the context of a missing person enquiry and the donor was content for it to be released for mitochondrial analysis in that country.

DNA PROFILES

287. DNA profiles are sometimes exchanged with foreign countries, though far less frequently than fingerprints. While fingerprints are usually exchanged to confirm a subject's identity, a DNA profile is usually exchanged in the hope of identifying the perpetrator of a crime. The Home Office's *International DNA Searching Policy for the United Kingdom* imposes very strict limitations on the circumstances in which profiles may be exchanged.

288. There are 4 types of DNA profile enquiry that are dealt with by the NCB.[113]

OUTBOUND SUBJECT PROFILES

289. The DNA profile of a known individual is sent abroad only with the express approval of a person of ACPO rank, after a risk assessment has been conducted, and with (for forces in England and Wales) the authorisation of the National DNA Database Strategy Board. Forces must explain why they believe that sending the profile to the specified country (or countries) is appropriate.

290. The Home Office's International DNA Searching Policy for the United Kingdom states that:

> *"1. A decision to release the DNA profile … of a known individual to an authority outside the UK must be made fairly, responsibly, with respect for the person whose profile is being released and without unlawful discrimination.*
>
> *2. A decision to release the DNA profile, sample and/or demographics of an identified individual may only be made if one or more of the following conditions is satisfied:*
>
> - *The release is for purposes related to the prevention or detection of crime;*
> - *The release is for the identification of a deceased person."*

Cases where subject profiles have been sent abroad are relatively rare: between January 2013 and September 2014 only 9 DNA subject profiles were sent abroad.

[113] Separately, the UK, the USA and Canada have an agreement to share DNA crime scene profiles only. Exchange is carried out via the Interpol secure electronic communication network. DNA subject profiles are not exchanged as part of this process.

INBOUND SUBJECT PROFILES

291. DNA subject profiles are received from abroad and sent to the NDU for searching against the NDNAD. The Home Office Policy states:

> *"The UK will only consider searching a DNA profile where the offence committed pertains to a UK Qualifying Offence (as defined by Section 7 of the Crime and Security Act 2010). ...*
>
> - *all requests for named person searches of the UK NDNAD will ... be considered on a case by case basis and may be referred for specific authorisation to the NDNAD Strategy Board;*
> - *only DNA profile searches received via a nominated authority will be undertaken;* and
> - *each search request received must be checked for a justifiable purpose to search the UK NDNAD (or Missing Persons DNA Database)."*

DNA subject profiles from other countries are received at a rate of approximately 2 per month.

OUTBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

292. Unidentified DNA profiles from crime scenes or from unidentified bodies or remains may be sent abroad for searching on another country's DNA database(s) at the request of the police force investigating the crime. The Home Office Policy states:

> *"The requesting force must be assured that:*
>
> - *the crime under investigation is a UK Qualifying Offence ...;*
> - *the DNA profile is retained on the UK NDNAD;*
> - *the crime stain material from which the DNA profile was generated is directly associated to the perpetrator of the crime ...; and*
> - *the investigation indicates a potential international link."*

DNA crime scene profiles are sent to other countries at a rate of around 4 per month; the comparable figure for profiles from unidentified bodies is fewer than one per month.

INBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

293. DNA crime scene profiles or unidentified body profiles may be received from abroad. The Home Office Policy states that an unidentified foreign crime scene DNA profile will only be searched against the National DNA Database if the relevant crime meets the definition of a 'UK Qualifying Offence' or with the approval of the Chair of the NDNAD Strategy Board. In each case consideration will be given to the question of whether or not there is a *"justifiable purpose to search the UK NDNAD (or Missing Persons Database)"*.

294. DNA crime scene profiles from other countries are received at a rate of around 30 per month; the comparable figure for profiles from unidentified bodies is around 2 per month.

FINGERPRINTS AND FINGERMARKS

295. There are 4 types of fingerprint enquiry dealt with by the NCB:

OUTBOUND FINGERPRINTS

296. This is the most usual type of fingerprint exchange and most commonly takes place where a UK force wants to send fingerprints abroad in relation to an arrest in the UK. It will usually want to do so because the person arrested is a foreign national or has foreign links and the force suspects that that person has engaged in criminal activity abroad. The force may already have sought (via ACRO) information about that person's foreign conviction history. Alternatively, the force may wish to send fingerprints abroad because the individual in question is a convicted sex offender who intends to travel to another country.

297. Any force which wants fingerprints sent abroad must explain why they think that there is a link to the specific country or countries to which the prints are to be sent. The force must also supply a risk assessment (signed by an Inspector for EU countries and by a Superintendent for non-EU countries) which addresses relevant Human Rights issues in the country or countries to which the fingerprints are to be sent.

298. Outbound fingerprint requests are processed at a rate of around 75 per month.

INBOUND FINGERPRINTS

299. Inbound requests occur when a foreign country sends fingerprints to the UK, for example to confirm identity.

300. Inbound fingerprint requests are received at a rate of around 4 per month.

OUTBOUND CRIME SCENE FINGERMARKS

301. Requests to send crime scene fingermarks to other countries are rarely made: certainly less often than once a month.

INBOUND CRIME SCENE FINGERMARKS

302. Inbound requests to search crime scene fingermarks against IDENT1 are received at a rate of around 2 per month. I understand that, as with crime scene DNA profiles, foreign crime scene fingermarks will only be searched against the UK database if the relevant crime meets the definition of a 'UK Qualifying Offence' and it is considered that "*there is a justifiable purpose to search*" IDENT1.

DIP SAMPLING

303. During a visit to the offices of the NCB in September of 2014 my Head of Office dip-sampled – and then reported to me on – 9 cases in which DNA profiles and/or fingerprints had been exchanged internationally. In 6 of those cases DNA profiles or fingerprints had been

transferred out of the UK. There was nothing about those cases which caused either of us any concern.

EUROPEAN ARREST WARRANTS

304. The NCB is also responsible for European Arrest Warrants (EAWs). EAW requests are received from other EU member states and often include the fingerprints of the relevant individual. These fingerprints are loaded onto IDENT1 so that identity can be confirmed on arrest. The fingerprints must be deleted from IDENT1 at the end of the process (i.e. once a decision is made regarding extradition or the EAW is cancelled).

305. For outgoing EAW requests, fingerprints relating to the subject are sent to the country in question using the Interpol secure electronic network. Those fingerprints must likewise be deleted from the receiving country's database at the end of the process.

306. It appears that in the calendar years 2010 to 2013 an average of approximately 240 EAW requests were made by the UK each year and that an average of approximately 5,670 EAW requests were received by it.[114]

POTENTIAL 'BIOMETRIC BREACHES'

307. There have been 3 occasions when the NCA and/or a police force have been proactive in drawing my attention to issues of possible concern as regards the international exchange of biometric material or data. Having looked further into these cases, I was satisfied that nothing unlawful had occurred; in 2 of them, however, I recommended that steps be taken to ensure that police and/or staff were alerted to the procedures that they should follow in future cases. I am grateful to the NCA and the relevant police force for bringing these cases to my attention.

PRÜM

308. The Prüm Council Decisions of 2008[115] provide for the automated 'bulk' exchange and cross-searching of DNA profiles, fingerprints and vehicle registration data among EU member states. The Prüm system covers both crime scene and 'reference' (i.e. individuals') DNA profiles and fingerprints/fingermarks and searches are conducted on an anonymised 'hit'/'no hit' basis. It has been suggested that considerable policing benefits could flow from UK membership of the Prüm system, particularly in circumstances where – as I have repeatedly been reminded – approximately 25-30% of individuals arrested by the MPS are foreign nationals. Equally, however, it has been suggested that issues arise as regards that system, particularly in the context of possible adventitious matches.

[114] See http://www.nationalcrimeagency.gov.uk/publications

[115] 2008/615/JHA and 2008/616/JHA

309. The Prüm Council Decisions are subject to the UK's opt-out under Protocol 36 of the Lisbon Treaty. On 10 July 2014 the Home Secretary stated[116]:

> *"the Prüm system … is about the easy, efficient and effective comparison of data when appropriate. We have been clear that we cannot rejoin that on 1 December and would not seek to do so. However, in order for the House to consider the matter carefully, the Government will produce a business and implementation case and run a small-scale pilot with all the necessary safeguards in place. We will publish that by way of a Command Paper and bring the issue back to Parliament so that it can be debated in an informed way. We are working towards doing so by the end of next year. However, the decision on whether to rejoin Prüm would be one for Parliament."*

I am aware in broad terms of the work that is underway in that connection and expect to be kept informed of its progress. I shall of course continue to take an active interest in that work and, in particular, in the terms and conduct of the proposed pilot exercise.

[116] See column 492 onwards at: http://www.publications.parliament.uk/pa/cm201415/cmhansrd/chan22.pdf

6. OTHER MATTERS

6.1 DNA PROFILING PROBLEMS

310. When DNA samples which have been taken from arrestees are submitted by forces to Forensic Science Providers (FSPs), DNA profiles are derived from those samples and loaded to the National DNA Database. In a small proportion of cases the FSPs are unable to derive profiles from the samples, usually because the sampling process (which involves the taking of 2 buccal swabs) has not been properly followed. In those circumstances the samples will be rejected by the FSPs and the police will have to take replacement samples if they want the arrestees' DNA profiles to be searched against the NDNAD.

311. During a visit to Thames Valley Police (TVP) in August of 2014, it was brought to my attention that since December of 2013 there had been a substantial increase in the number of cases where Cellmark, the FSP most often dealt with by TVP, had rejected DNA samples which TVP had submitted for profiling. This increase was apparently attributable to fibrous contamination of the samples (swabs) at issue. TVP had employed an independent forensic fibre expert to determine the source of the contamination and a copy of the resulting report was made available to me. The report records that 48 unused sampling kits were examined and that approximately 70% of the swabs that were tested were found to be subject to at least some degree of fibrous contamination.

312. The Home Office has been aware of this problem since February of 2014 and has collected data about sample rejection rates. Although it seems that other forces and FSPs have reported no significant rise in those rejection rates, it is recognised that this may be due to the differing 'quality parameters' which FSPs apply. Cellmark has now amended its processing procedures to take account of the presence of fibres in some samples and I understand that its rejection rates have fallen substantially. Cellmark has apparently confirmed, however, that the number of fibres found in samples is not decreasing.

313. My main concern on being notified of this issue was that it might raise doubts as to the integrity of profiles on the NDNAD. It has apparently been established, however, that any fibrous contamination of buccal swabs in DNA kits has occurred while the swabs are being manufactured. After swabs are manufactured, they are then treated to remove any traces of DNA. As any fibres will already have been on the swabs at this stage, any fibres in the kits received by forces will also have been treated. In those circumstances the NDNAD Delivery Unit is satisfied that there is no risk to the integrity of the database.

314. As a result of this 'fibre contamination' issue, profiles which should have been loaded to (and searched against) the NDNAD have either never been loaded to it or have been loaded only after replacement samples have been taken. Since, moreover, that issue is still ongoing, it remains the case that some profiles are not being produced and that there is a

continuing risk that the individuals in question may no longer be traceable if/when the police attempt to obtain replacement samples from them.

315. I shall continue to make enquiries into these matters. In the meantime I have asked for – and expect soon to receive – a full report from TVP about the impact of this issue on it, about the number of cases where it has sought to re-sample arrestees, and about the degree to which that exercise has been successful. I have also asked to be kept abreast of further developments as regards the wider contractual and procurement issues that arise.

6.2 FINGERPRINT GOVERNANCE ARRANGEMENTS

GENERALLY

316. While the governance arrangements as regards the National DNA Database are clear and comprehensive, those as regards IDENT1 are at best opaque. It has been suggested to me that this is because a variety of bodies – the Home Office, ACPO, the Police Information Technology Organisation and the National Policing Improvement Agency – have from time to time had or shared responsibility for the development and operation of a searchable national fingerprint database for police use. Whatever the explanation – and though I have seen nothing to suggest that the current arrangements have given rise to impropriety – there is a surprising lack of clarity as to where ultimate responsibility and accountability lie for the integrity and proper operation of IDENT1.

317. Equally, while it appears to be accepted by all concerned that the NDNAD Strategy Board has the right and duty to exercise general oversight and control over the collection and processing of DNA samples for forensic use, I have been unable to identify a group or body that performs a similar role – or is perceived to have similar authority – as regards fingerprints.

318. I recognise, of course, that the challenges that arise in relation to forces' retention and use of fingerprints are very different from those that arise in relation to their retention and use of DNA, not least because:

- issues of judgment and interpretation arise much more frequently in the context of fingerprints, particularly as regards the matching of crime scene marks to individuals;

and because

- there are numerous local police fingerprint bureaux and databases.

Even so, the fact that the forensic fingerprint world lacks both clear governance arrangements and a body of comparable status to the NDNAD Strategy Board is in my view – and as stakeholders have been quick to accept – a real and important weakness.

319. Steps are now being taken to address that weakness, particularly by a Fingerprint Governance Group which has been set up by Chief Constable David Shaw, the relevant

ACPO lead. I attend the meetings of that Group and in recent months it has set about the task of establishing a body that is in at least some ways analogous to the NDNAD Strategy Board. Although there continue to be differing views as to the precise responsibilities that that body should discharge, I am hopeful that real progress will soon be made in addressing the uncertainties that currently exist as regards governance and oversight in this area. I am also hopeful that, by the publication of annual reports, such a body will provide the public with improved access to information about police fingerprint databases and about the contribution they make to the prevention and detection of crime.

IDENT1 AND IABS

320. The difficulties that arise as regards fingerprints governance are compounded by the fact that:

- it is intended that the current IDENT1 service should be replaced within the next few years and that the successor service should deliver 'improved biometric capabilities' including capabilities in respect of other biometric information such as facial images and iris recognition; and
- it is also intended that that new system should 'converge' with the Immigration and Asylum Biometric System ('IABS').

Those difficulties are also compounded by the fact that, as the current IDENT1 contract expires on 31 March 2015, work on that larger project has to be combined with the development of an 'interim solution' which will provide continuity of service in the meantime.

321. It is obviously important that in this context – as in other contexts – careful consideration continues to be given to the governance issues that arise, not least as regards the sharing of biometric information among organs of the state. I shall of course take a close interest in the progress of those projects and expect to be alerted to any developments that are of relevance to my areas of responsibility.

322. Whereas the Unified Collection on IDENT1 now contains the fingerprints of around 7.7 million individuals, the IABS database contains the fingerprints of around 12 million visa applicants and others. As one would expect, there has long been a process whereby it has been open to the police to search arrestees' fingerprints against those held on IABS and for the relevant immigration and asylum authorities to make searches against IDENT1. In large part this is done via the Police Immigration Fingerprint Exchange ('PIFE') interface and I understand that that process has made a considerable contribution to the detection of crime (e.g. in the context of 'Operation Nexus') and to the protection of UK borders. I have seen nothing to suggest that there is or has been any impropriety in this cross-checking process.

323. Although I have no statutory functions as regards IABS I have had a number of meetings with those who are responsible for that database, particularly about the (actual and planned) retention of fingerprints and photographs on it.[117] I am impressed by the thoughtful and consultative approach they are adopting towards those issues and am grateful to them for the information they have provided to me.

6.3 ENQUIRIES AND THE PROVISION OF INFORMATION

REQUESTS FOR INFORMATION BY MEMBERS OF THE PUBLIC

324. My Office has received a range of enquiries about matters in relation to which I have no remit. They include enquiries about matters as diverse as ancestry, civil fingerprinting in the workplace and schools, and biometric enrolment for visa purposes. Enquiries about immigration and visa matters have been particularly frequent and accounted for exactly half of the 144 written enquiries from members of the public which had been received by my Office by 31 August 2014. I have raised with officials from the UK Visas and Immigration department of the Home Office the accessibility of information about such matters and the visibility of contact details for their teams.

325. More importantly, my Office has received a number of queries from concerned members of the public requesting information about, and/or confirmation of, the deletion of their biometric records from national and police databases. Whilst it would have been inappropriate for my Office to provide any form of legal advice to those individuals, in each of those cases my staff have sought to inform them about the new PoFA regime, about the circumstances in which biometric records may be retained, and about the circumstances in which deletion is likely to have taken place automatically. Where appropriate, my Office has advised the individuals concerned to make a Subject Access Request (pursuant to the Data Protection Act 1998) to the police force responsible for taking the fingerprints and/or DNA sample at issue with a view to obtaining the confirmation they desire.

326. Together with others from my Office I have spent a great deal of time in the past year liaising with representatives of the Home Office, Police, ACPO, ACRO and the Security Services about Subject Access Requests and the making of appropriate disclosure when requests are made by members of the public for information about biometric material which may or may not be being held by police forces. I have been surprised at how difficult it has proved to make progress on these matters and at the time it has taken for properly informative 'standard form' responses to be formulated.

[117] The immigration and asylum authorities – like the passport authorities – hold large databases of photographs.

327. During this process, which began before the commencement of the relevant legislative provisions, my Office has made a number of suggestions and recommendations and has repeatedly pressed for a speedy resolution of the issues which have arisen. In spite of the time and resources that have been expended, however, it seems that standard wordings have yet to be finalised and, in the light of the most recent drafts that I have seen, I remain unconvinced that the general public will understand or be sufficiently reassured by the wording of the responses that they may receive to Subject Access Requests.

328. I consider it very important that the police's dealings with the public on the issue of retained biometrics are as transparent as they can be and as fair as possible to the individuals concerned. I shall therefore be actively pursuing this matter.

REQUESTS FOR INFORMATION BY THE POLICE

329. I have received a number of requests for information and advice from police forces as they attempt to negotiate the complexities of the new retention regime and, in particular, the ways in which it affects their legacy and 'cold case' investigations. Two cases raised the issue of whether and how hard copies of fingerprints which had been retained in a case file could be used by investigators after the electronic fingerprint records on IDENT1 had been deleted during the 'bulk' deletion process which took place prior to the commencement of PoFA. In both those cases – as in others – it would not have been appropriate for me or my Office to give legal advice to the forces concerned and they were told that they should consult the CPS and/or their in-house lawyers as a matter of urgency. We were, however, at least able to alert those forces to some of the issues which arose for consideration and, I hope, usefully to inform their thinking about those issues.

330. I am, of course, keen to be told of any concerns or practical problems that arise in the context of the new retention regime so that I can, where appropriate, pursue them.

FOI REQUESTS

331. Since my appointment I have received – and have declined to respond to – three FOI requests. I have no obligation to respond to such requests as neither I nor my Office appears in the list of public authorities at Schedule 1 of the Freedom of Information Act 2000.[118]

6.4 RESEARCH

332. Since my appointment I have repeatedly made clear to Home Office officials and others that I consider it highly desirable that, as regards the new retention regime introduced by PoFA, there should be proper data collection and research such as will inform policymakers and others as to the effectiveness and proportionality of that new regime and as to whether the

[118] http://www.legislation.gov.uk/ukpga/2000/36/schedule/1.

relevant 'lines' have been drawn in the right place. By the beginning of 2014 it had become clear that the Home Office had no plans to conduct detailed research in this connection.

333. Around that time I entered into discussions about this research issue with Home Office officials and with academics from the Universities of Northumbria and Durham. A number of ideas and proposals were discussed, and it seemed that there were at least four possible – and in various ways overlapping – areas of desirable research.

    i. Research which was aimed at establishing – by reference to a proper evidence base – the parameters of a sensible and proportionate retention regime for biometric material.

    ii. A variant or subset of that sort of research i.e. research into the true usefulness of biometric information in the police/criminal justice system process.

    iii. Research which was aimed at comparing the effectiveness/usefulness of the English and Welsh retention regime and databases with that/those of other countries.

    iv. Research which was aimed at establishing the impact of the changes made by PoFA – especially on the value and usefulness of the DNA and fingerprint databases.

    Research of any of those types would no doubt be welcome. It seemed to me, however, that, for the purposes of my own role, research of the fourth type might well be the most manageable, informative and useful.[119]

334. I proposed in February of 2014 that the relevant academics and Home Office officials should make contact with each other and that all of us should then meet to discuss the various research options. In March of 2014, however, I was told that it had been decided that, before any such meeting took place, it would first be necessary to alert ministers to the matter and to obtain their consent to the sort of disclosure that would be required in the context of a research project. Although I have repeatedly sought to take the matter forward since that date – and although others (such as the Chair of the NDNAD Strategy Board) have repeatedly made clear that they are also of the view that a proper post-implementation review of the PoFA retention regime is required – no further progress appears to have been made.

335. I understand that the Home Office considers that recent 'match rate' data as regards the National DNA Database suggests that the introduction of the PoFA retention regime has not led to a reduction in the effectiveness of that database. In my view, however, it remains obviously desirable that proper – and ideally independent – research should be conducted into the impact of that new regime and I intend to continue pressing for such research to be carried out.

[119] Such research would, of course, cover – but by no means be limited to – the issues which are referred to at paragraphs 114, 115 and 119 above.

7. CUSTODY PHOTOGRAPHS AND FACIAL RECOGNITION TECHNOLOGY

336. Although my statutory responsibilities as Biometrics Commissioner relate (like the relevant provisions of PoFA) only to DNA and fingerprints, I am conscious that the term 'biometric data' is usually thought to include facial images and voice patterns. I am also conscious:

- that in the last few years there have been substantial developments in automated facial recognition systems – and, indeed, in automated speaker recognition systems – and that such systems could well be of real value to the police in the prevention and detection of crime;
- that no other commissioner or regulator appears to have a remit which specifically covers the use of such systems by the police;
- that the issues and concerns which have arisen as regards the retention and use by the police of DNA and fingerprints are very similar indeed to those which have arisen, and seem likely to arise, as regards the police's retention and use of facial images in general and of custody photographs in particular;[120] and
- that the same may well be or become true of speaker recognition systems.

Against that background, I have taken an active interest in the work that is being done by law enforcement agencies in these fields and have, in particular, had numerous dealings in that connection with police forces, with Home Office officials and with others.

337. In January of 2014 I became aware that the police were actively investigating the possibility of uploading custody photographs to the Police National Database ('the PND') and of applying automated facial recognition technology to those images. I asked to be kept abreast of developments in that connection and of any relevant pilot testing. At the beginning of April of 2014 I was invited to attend a meeting in Durham of the ACPO Facial Recognition Working Group. At that meeting I was informed that some 12 million custody photographs had been uploaded to the PND and that an automated searching mechanism had 'gone live' five days previously.

338. On 7 April 2014 I wrote to the chair of that Working Group (Chief Constable Michael Barton of Durham Constabulary) to draw formally to his attention *"my concerns about problems which, in my view, may well arise as a result of what appears to have been a decision to put the database and searching mechanism into immediate operational use"*. In that letter I made the following points.

[120] It will be appreciated that, just as those who are arrested by the police are usually required to provide them with their fingerprints and a DNA sample, so are they usually required to provide them with a 'custody photograph'.

There are a number of concerns which might sensibly arise in connection with the work and proposals which were discussed at the meeting. They include concerns about such matters as:

- the acceptability of creating what is, in effect, a searchable national database of custody photographs;
- the inclusion and processing on that database of images of individuals who have never been convicted of a recordable offence;
- the scope for searching against that database other images of unconvicted individuals (including, perhaps, images derived from CCTV and/or 'body worn video');

and, more generally, about

- what would constitute appropriate arrangements for the governance and regulation of the relevant database and searching process.

My concern at this stage arises out of the fact that a searchable national database of custody photographs has, it seems, been put into operational use before any of those issues have been resolved. In particular, it appears to me that difficult legal, political and other problems may well quickly arise as regards:

- the inclusion and processing on that database of images of individuals who have never been convicted of a recordable offence; [the retention of such images has, in connection with custody photographs, already given rise to litigation in the English Courts in *R (RMC and FJ) v MPS* [2012] EWHC 1681 (Admin)] and
- the apparent absence of any very rigorous testing of the reliability of the facial matching technology that is being employed.

More generally, I am concerned as to whether it can really be appropriate for the police to put into operational use without further consultation a searchable database of custody photographs which is subject to none of the controls and protections which apply as regards the national DNA and fingerprint databases by virtue of the Protection of Freedoms Act 2012.

It would appear to be particularly difficult to justify the indefinite retention of photographs where they are *"entered on and held in a searchable database which has been systematically compiled"* [see e.g. *S & Marper v UK* [2008] ECHR 1581 (at para 82) and *R (Catt) v ACPO etc* [2013] EWCA Civ 192 (at paras 9 and 12)].

I am acutely conscious of the importance of this 'facial imaging' project and of the contribution it may make to the prevention and detection of crime. I am keen to assist that project in any way that I reasonably can. In all the circumstances, however, I have real doubts as to whether it can be wise at this stage – and without wider consultation and specific legal advice – to continue with the proposed operational use of the new system.

339. In his helpful response to my letter – and whilst, among other things, expressing the view that *"photographic searches are substantially different to DNA and fingerprint searches"* – CC Barton made clear that he was *"alive to the civil liberties and wider freedoms issues which are part of the PND work"* and suggested that we meet again to discuss my concerns and wider issues. In the event, however, that suggestion has been superseded by later developments and, in particular, by the involvement of others in that 'PND work'.

340. Since writing my letter of 7 April I have been actively pursuing the concerns which I raised in it with senior Home Office officials and with others. Although I have been doing so both in correspondence and at meetings – and although I have repeatedly been assured, and entirely accept, that those officials have been taking active steps to ensure that those concerns are properly addressed – I have as yet seen little to suggest that significant progress has been made in relation to them. As things stand at present, then, it seems:

- that several million custody photographs – including those of hundreds of thousands of individuals who have never been charged with, let alone convicted of, an offence – have been loaded to the PND and that more are being loaded to it each day;
- that this has been and is being done notwithstanding the fact that, in the light of the judgment in *R (RMC and FJ) v MPS*, it seems likely that many of those images should no longer be being held by the police;[121]
- that the uploaded images are being subjected to a searching mechanism – of, at best, questionable efficiency – whereby uploaded images (whether from CCTV or some other source) are compared to the archived custody photographs;
- that although a searchable police database of facial images arguably represents a much greater threat to individual privacy than searchable databases of DNA profiles or fingerprints, this new database is subject to none of the governance controls or other protections which apply as regards the DNA and fingerprint databases by virtue of PoFA; and
- that this new database and searching technology has been put into operation without public or Parliamentary consultation or debate.

[121] In *R (RMC and FJ) v MPS* the two claimants, neither of whom had been convicted of an offence, sought the destruction of, among other things, their custody photographs. The Court held that the retention of those photographs "*in application of the existing [national police] policy*" amounted to an unjustified interference with their right to respect for their private lives and that that policy was unlawful. The Court decided, however, "*to allow the defendant a reasonable further period within which to revise the existing policy, rather than to grant relief that might have the effect of requiring the immediate destruction of the claimants' photographs without the possibility of re-assessment under a revised policy*". It also observed that "*it should be clear in the circumstances that a 'reasonable further period' for revising the policy is to be measured in months, not years*."

In the event – and although more than two years have passed since judgment was given in that case – it would appear that no 'revised policy' has in fact been brought into existence as regards the retention of custody photographs and that many (and perhaps most) police forces in England and Wales continue to follow a policy of retaining almost all custody photographs for an indefinite period regardless of whether the individuals concerned have or have not been convicted of an offence.

341. It is further apparent from my enquiries that, quite apart from this new national database, facial matching technology is also being applied to searchable local police databases of custody (and possibly other) photographs. In particular, there have been a number of media reports about the use of such technology by Leicestershire Police[122] and I have myself had discussions with representatives of the Metropolitan Police Service about the work that it has been doing in that connection. It is my impression that the MPS – which was, of course, the defendant in *R (RMC and FJ) v MPS* – is fully alert to the issues that arise as regards such searchable databases and to the need to ensure that they do not include custody photographs which cannot lawfully be retained.

342. I of course recognise and welcome the contribution that the application of automated facial and speaker recognition systems to appropriate police databases can make to the prevention and detection of crime and to the protection of public safety. I also recognise that there is scope for differing views as to the appropriate regulation of such systems and databases and, in particular, that it may be that a different regulatory approach should be taken to them than that which is laid down by PoFA for DNA profiles and fingerprints. In my view, however, proper consideration should now be given to the civil liberties and other issues that arise as regards those newer technologies and urgent steps should now be taken to ensure that they are governed by an appropriate regulatory regime. In the absence of such steps there must be a real risk that the considerable benefits that could be derived from the use of these new technologies will be counterbalanced by a lack of public confidence in the way in which they are operated by the police and/or by challenges as to their lawfulness.

343. As well as raising my concerns about these matters with Chief Constable Barton and with senior Home Office officials, I have raised them with the Forensic Science Regulator, with the Surveillance Camera Commissioner and with the Information Commissioner's Office. It is clear from my discussions with them that they also have concerns about proper regulation in this area and that they would, like me, be happy to contribute to the development of an appropriate regulatory regime.[123]

344. It has for some time been my intention to raise the above issues in this report. Given their importance, however, and their obvious relevance to an inquiry launched by the Parliamentary Science and Technology Committee into *"the potential use and collection of biometric data and whether regulations in this emerging field are adequate"*,[124] I have

---

[122] See e.g. http://www.itv.com/news/central/2014-07-15/facial-recognition-first-for-leicestershire-police/ and http://www.bbc.co.uk/news/uk-england-leicestershire-28307938?print=true

[123] I have, moreover, raised some of my concerns with Her Majesty's Inspectorate of Constabulary, particularly about the retention policies which appear to be being applied by some police forces in relation to custody photographs. As yet, however, I have done so only in outline.

[124] http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/

already raised them in almost identical terms in a written submission to that Committee. In that written submission – and in response to a specific question posed by the Committee – I observed:

> *"In summary, then, a key and pressing challenge facing Government in connection with new technologies that rely on biometric data is, in my view, the development of an appropriate regulatory regime as regards the application of automated facial recognition technology to police databases of custody photographs. A sensible way of addressing those challenges would be for Government to bring forward proposals for such a regime and to put them out for public consultation. One obvious possible model for such a regime would be that which already applies to DNA profiles and fingerprints."*

I remain of that view.

8. RESOURCES, ACCOMMODATION AND WEB PRESENCE

8.1 STAFFING

345. My Office currently includes 3 members of staff in addition to myself:

- a Head of Office (who took up post in April of 2013);
- a Policy and Casework Manager (who took up post in June of 2013); and
- a Caseworker (who took up post in January of 2014).

I also have access to independent media advice and have made arrangements to obtain independent legal advice if and when that proves to be necessary in the context of litigation.

346. I have concluded that, if I am to discharge my statutory functions properly, I will require the assistance of an additional caseworker. Although this has long been acknowledged by the Home Office and although I have long had approval for the recruitment of such a person, it now appears that that post will remain unfilled for the duration of a recently-announced Home Office recruitment freeze.

347. The legislation makes no provision for the appointment of a 'Deputy Commissioner' or for the appointment of any other person to whom I may delegate my decision-making powers. It occurs to me that a situation could arise where I am incapacitated and thus unable to make a decision on an application under section 63G or in respect of an NSD, or where it would be improper for me to do so because I have some association with the subject of the application or NSD. I am investigating the possibility of arrangements being put in place to cater for such a situation.

8.2 EXPENDITURE

348. Before I took up post I repeatedly sought reassurance that I would be provided with sufficient resources to enable me properly to discharge the responsibilities of the role. It was acknowledged by the Home Office that we were "*in the frustrating position of not knowing the precise resource requirements before the Protection of Freedoms Act provisions [came] into force*" and I was assured that, with a view to ensuring that the role was a success, the Home Office would "*keep under regular review the level of resourcing provided – both in terms of the size and skills of the Commissioner's Office, the support provided by the Home Office, and the Commissioner's own time*."

349. When I took up my role in March of 2013 I was allocated a budget of £250,000 and given approval to recruit a 'Grade 7' and an 'Executive Officer' (EO) for my Office. Although I duly recruited a Grade 7 (who became my Head of Office in April of 2013), no EO was recruited at that time. In May of 2013 it was agreed that it would be more appropriate to recruit 2

'Higher Executive Officers' (HEOs) rather than a single EO and my budget was accordingly increased to £290,000. Although an HEO was duly recruited and became my Policy and Casework Manager in June of 2013, I decided not to recruit a second HEO until it was clear that – and when – one would be required.

350. I was originally appointed on the basis that my services would be required for only the equivalent of three days per week. In anticipation of the coming into force of PoFA on 31 October 2013, however, it was recognised that a greater time commitment would be required of me and in September of 2013 it was agreed that from November or December of 2013 I should move to full-time working. It was also agreed that, rather than recruiting a second HEO, I should recruit 2 EOs as caseworkers. I began working full-time at the beginning of December 2013 and an EO took up post as a caseworker in January of 2014. As is indicated above, a second EO has yet to be recruited.

351. My Office's expenditure during the financial year 2013/14 was as follows:

Salaries:	223,120
Accommodation and associated expenses:	50,372
Travel and Subsistence:	2065
Stationery, PO box, telecoms etc.:	1159
Total:	276,716

352. In February of 2014 I was notified that my Office's budget for 2014/15 would remain at £290,000. As I pointed out, such a sum would have been insufficient to cover the current costs of my Office and would have given rise to a considerable shortfall if and when, as had been agreed should happen, a second caseworker was recruited.

353. I subsequently had various meetings and exchanges of correspondence with officials from my sponsoring departments within the Home Office and it has now been agreed that my Office's budget for 2014/15 will be £300,000. For a number of reasons – including in particular the recruitment freeze that is referred to above – it seems likely that that budget will be underspent.

8.3 ACCOMMODATION

354. Although a central feature of my post is that it is – and must be seen to be – independent of government, my Office is accommodated within the Home Office estate i.e. the estate of a department we oversee. Due to the reorganisation of that estate my Office has been required to move twice since June 2014. We have recently been relocated to office space

which appears to suit our accommodation needs more closely than that which was previously available to us: however, this remains within the Home Office HQ building and there is no physical restriction on access to that space by ordinary Home Office staff.

355. Whilst I am grateful for the efforts that have been made to meet our accommodation needs, I am not convinced that the current arrangements will prove sufficient in the longer term. Quite apart from the difficulties which continue to arise as regards perceived independence:

- it is not clear that sufficient space will be available to us if/when an additional caseworker is recruited; and
- sensitive national security systems to which we need access are housed in a shared office in a separate section of the building and the relevant secure accommodation (one desk in a shared office) does not allow for more than one member of my Office to work there effectively.

356. As with the budgetary position as regards my Office, I will of course keep under review the suitability of the accommodation that is made available to it.

8.4 WEB PRESENCE

357. One of my main concerns when I accepted the role of Biometrics Commissioner was that I should not only be, but that I should be seen to be, independent of government. In that connection I have made clear since before my appointment that I consider it important that I have a wholly independent website. An exemption was required from the Government Digital Service (GDS) within the Cabinet Office to allow me to set up a secure website outwith the ambit of the GOV.UK website.

358. Over a period of some months repeated efforts to secure such an exemption were made on my behalf by Home Office officials and by my Office. Other independent Commissioners and bodies have been successful in obtaining exemptions but in my case an exemption was refused on the grounds that the relevant criteria were not met. Remarkably, the document which sets out those criteria expressly provides that "*the need to appear independent is not sufficient grounds for an exemption* ... ." On 27 August 2013 I wrote to Lord Taylor to make him aware of the situation and of my dissatisfaction with it: I made clear, however, that I was not at that time inclined to ask him or the Home Secretary to intervene in the matter.

359. Currently, therefore, my Office's only web presence takes the form of a page on the GOV.UK website: www.gov.uk/biometrics-commissioner. On this page, the public can find information about what my Office does together with links to relevant legislation and documentation. While in the main I am satisfied that the GOV.UK website allows the public to access the information they need regarding my role and my Office, I find the inflexibility of approach on that website restrictive in terms of content, style and form, and I consider

the rules that prevent me, as an independent Commissioner, from having an independent web presence, deeply unsatisfactory.

LIST OF ACRONYMS

ABH	Actual Bodily Harm
ACPO	Association of Chief Police Officers
ACPO TAM	Association of Chief Police Officers, Terrorism and Allied Matters
ACRO	Association of Chief Police Officers Criminal Records Office
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CTA	Counter-Terrorism Act 2008
CTFS	Counter Terrorism Forensic Services
EAW	European Arrest Warrant
ECtHR	European Court of Human Rights
FOI request	A request under the Freedom of Information Act 2000
FSPs	Forensic Service Providers
GBH	Grievous Bodily Harm
GDS	Government Digital Service
IABS	Immigration and Asylum Biometric System
IDENT1	The national police fingerprint database
JCHR	Joint Committee on Human Rights
JFIT	Joint Forensic Intelligence Team
MOU	Memorandum of Understanding
MPS	Metropolitan Police Service
NCA	National Crime Agency
NCB	National Crime Bureau in the NCA
NDNAD	National DNA Database
NDU	NDNAD Delivery Unit
NFA	No Further Action

NSD	National Security Determination
OBC	Office of the Biometrics Commissioner
PACE	Police and Criminal Evidence Act 1984
PIFE	Police Immigration Fingerprint Exchange
PNC	Police National Computer
PND (*a* or *the*)	*A* Penalty Notice for Disorder or *the* Police National Database
PoFA	Protection of Freedoms Act 2012
PSNI	Police Service of Northern Ireland
SCC	Serious Crimes Cache
SPOC	Single Point of Contact
TACT	Terrorism Act 2000
TPIMs Act	Terrorism Prevention and Investigation Measures Act 2011
TVP	Thames Valley Police
UKAS	United Kingdom Accreditation Service

ISBN 978-1-4741-1331-1