ANNUAL REPORT 2015

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Alastair R MacGregor QC

December 2015

Office of the Biometrics Commissioner

ANNUAL REPORT 2015

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

March 2016

Any enquiries regarding 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 9781474129350
Web ISBN 9781474129367

ID 24021602 03/16 54496 19585

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 second 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.

This Report is intended to be comprehensible to a reader who is unfamiliar with my 2014 Report and I have therefore repeated in it some of the background and explanatory information that was contained in that earlier report. In some places, however, I have simply referred the reader to relevant passages in that report. A copy of it can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387601/45428_Biometrics_Annual_Report_ACCESSIBLE.PDF.

The structure of this Report is similar to that of my 2014 Report and 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 the Protection of Freedoms Act 2012 (PoFA) and which came into effect on 31 October 2013. 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 and the principles that I apply when deciding such applications;
- the development and nature of the application and decision-making processes;
- 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 number, nature and outcome of the applications for extended retention that were made between 31 October 2013 and 31 August 2015 (paragraphs 31-64);
- concerns that have arisen as regards:
    - the taking and retention of biometric material from those who have been convicted of qualifying offences outside England and Wales; and
    - the absence of substantive progress in that connection since I expressed those concerns in my 2014 Report (paragraphs 68-83);
- the limited extent to which forces other than the Metropolitan Police have engaged with the application process, the risks that arise in that regard, and the reasons why

forces may consider that those risks are reasonable ones for them to run (paragraphs 97-106); and

- points which Parliament may wish to bear in mind if and when it gives further consideration to that process (paragraphs 107-109).

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 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:

- concerns that have arisen:
    - as a result of procedural problems and handling delays in relation to New Material (i.e. biometric material which has been collected since 31 October 2013) (paragraphs 142-146 and 159); and
    - as regards the timely destruction/deletion of such material (paragraphs 167-168);
- the development of 'emergency' or 'holding' NSDs (paragraphs 147-151);
- a statistical overview of holdings on the CT databases and of the operation of the NSD process between 31 October 2013 and 31 October 2015 (paragraphs 154-158); and
- the handling of – and the governance arrangements that apply to – biometric material in the context of CT-related matters (paragraphs 165-170).

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 '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 DNA samples by Forensic Science Providers and police forces, the compliance checks that have been and will be carried out, and the number of DNA samples held under the CPIA exception;
- the deletion of 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 process 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:

- recent changes as regards:
    - the retention of 'elimination' samples pursuant to the CPIA exception (paragraphs 186-188); and
    - the obtaining of properly informed consent from individuals who provide biometric material for elimination purposes (paragraphs 189-190); and
- issues relating to the programming and operation of the PNC – and to the release of arrestees otherwise than on bail – 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 214-243 and 251-253).

In **Section 5** I deal with the use to which biometric material is being put. In particular I deal with 'unlawful matches' (i.e. matches with unlawfully held material), 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:

- concerns that have arisen about the policies which some forces have adopted as regards unlawful matches (paragraphs 263-267);
- ongoing concerns about issues relating to the operation of the speculative search process, especially as regards fingerprints (paragraphs 268-275);
- the introduction of a new policy governing the international exchange of DNA profiles and associated demographic information (paragraphs 278-279); and
- the recent decision that the UK should opt in to the Prüm mechanism which allows for the automated cross-searching of DNA profiles and fingerprints among EU member states (paragraphs 315-318).

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

- the Government's proposed Biometrics Strategy and the Home Office Biometrics Programme;
- fingerprint governance arrangements;
- the oversight of biometric retention in Northern Ireland; and
- the desirability of proper research into the impact of the retention regime introduced by PoFA.

Matters of particular significance which are addressed in that section (and, indeed, in Section 7) include the increased scope for the sharing of biometric information among organs of the state and the need for proper governance and regulation in that connection (paragraphs 319-322 and 329).

In **Section 7** I deal, as I did last year, with my concerns about the establishment and operation of a national police database of custody photographs to which facial recognition technology is applied. In that section I summarise – and express concern about – the limited progress that has been made in relation to those matters notwithstanding the announcement of a Home Office review in December of 2014 and the observations made by the House of Commons Science and Technology Committee in March of 2015.

In **Section 8** I deal with my Office's resources, accommodation and web presence and with the upcoming expiry of my term as Biometrics Commissioner.

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 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 **18 December 2015**

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 BIOMETRIC REGIME INTRODUCED BY POFA

7. Put shortly, what Parliament in essence decided when it introduced the 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 DNA profile has been derived from it and in any event within six months of the date it was

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

[3] See e.g. paragraphs 119 and 125 of the Judgment.

[4] See Part 1 of Schedule 10.

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 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.

---

[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 section 65B of PACE and section 65 of the Crime and Disorder Act 1998.

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

In both those cases, moreover, that three-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 POFA 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 that, despite those deletions and the more restrictive retention regime that has been in place since October of 2013, some 12.5% of men and some 3% of women in the United Kingdom continue to have their DNA profiles and/or fingerprints retained on those national databases. It should also be noted that, contrary to what many appear to have feared before that more restrictive regime was introduced, its introduction seems to have had no demonstrably adverse impact on the overall effectiveness of the databases. Indeed, it seems that the overall 'match' rate on the National DNA Database has in fact risen.[10]

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.

---

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

[10] See the National DNA Strategy Board's 2014/15 Report at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484938/52921_NPCC_National_DNA_Database_print_ready.pdf (especially at Section 1.3).

17. In those circumstances it was quickly decided that the only sensible way of putting the PoFA 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 by no means been problem-free.

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 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.[11]

    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.[12]

    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.[13]

    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.

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

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

[13] 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[14]

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,[15] 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.[16]

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.*

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

[15] 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.

[16] 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.[17] While 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 usually be informed of any application for extended retention and given the opportunity to make representations against it,[18] 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.

CORE PRINCIPLES AND RELEVANT FACTORS

23. Having carried out the consultation exercise described in my previous Report,[19] the approach which I decided to adopt to applications under section 63G(2) and (3) is as 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.

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

[18] Further relevant provisions are at sections 63G(7) to (9).

[19] (at paragraph 23)

"Core Principles

...

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.

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."

OTHER DOCUMENTS

24. In addition to that *'Principles*' document, my Office and I have 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. Furthermore (and as was contemplated by section 24 of PoFA) formal guidance about such applications has been issued and published by the National DNA Database Strategy Board. That guidance is consistent with the

'Principles' and other documents that have been issued by my Office and a copy of it 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'

25. By section 63E of PACE (as amended by 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.

26. 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 specific 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.

    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 (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 the 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 the 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.[20]

27. 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.

28. 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 – usually 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 almost always be deleted automatically.[21]]

PROCEDURE AND PROCESS

29. 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.[22]

30. As fairness clearly requires, reasons are given for every decision that I make on an application under section 63G. Any such decision may be subject to Judicial Review on the

[20] Exceptions to that general rule are discussed at paragraphs 56 and 240-243 below.

[21] Cases where this does not happen are referred to at paragraphs 56, 227-228 and 240-243 below.

[22] Further information about the casework process which is currently adopted within the OBC – and a flowchart which illustrates it – can be found at paragraph 36 of my 2014 Report. Every force has been asked to nominate a single point of contact (a 'SPOC') to be responsible for co-ordinating applications to me under section 63G and my Office and I are always happy to answer questions from forces about the scope for such applications and about the application process.

application of either the individual affected or the applying officer. As yet, no applications for Judicial Review have been made and no 'Pre-Action Protocol' letters have been received.

2.2 APPLICATIONS RECEIVED

VOLUMES

ESTIMATES

31. 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.

32. 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

33. In the event, however, the number of applications which I have actually received has been substantially lower than was estimated. In particular, in the first 22 months after the relevant sections of PoFA came into force on 31 October 2013 (i.e. in the period to 31 August 2015) only 209 applications were received.

34. Of those 209 applications:

- 91 were made in the period 31 October 2013 to 31 August 2014; and
- 118 were made in the period 1 September 2014 to 31 August 2015.

It will be observed that the average rate of applications in this current reporting year (i.e. between 9 and 10 per month) has been broadly consistent with that in 2013/14. It should also be noted that the great bulk of the 209 applications (i.e. 88 of the 91 in 2013/14 and 107 of the 118 in 2014/15) have been made by the Metropolitan Police Service ('the MPS') and that only 8 of the other 42 forces in England and Wales have made applications to me.[23]

[23] In the 10 months to 31 August 2014 the City of London, Durham and West Mercia forces each made a single application. In the 12 months to 31 August 2015 applications were made by Cambridgeshire Police (2), Greater Manchester Police (3), Kent Police (1), Northumbria Police (4) and West Yorkshire Police (2).

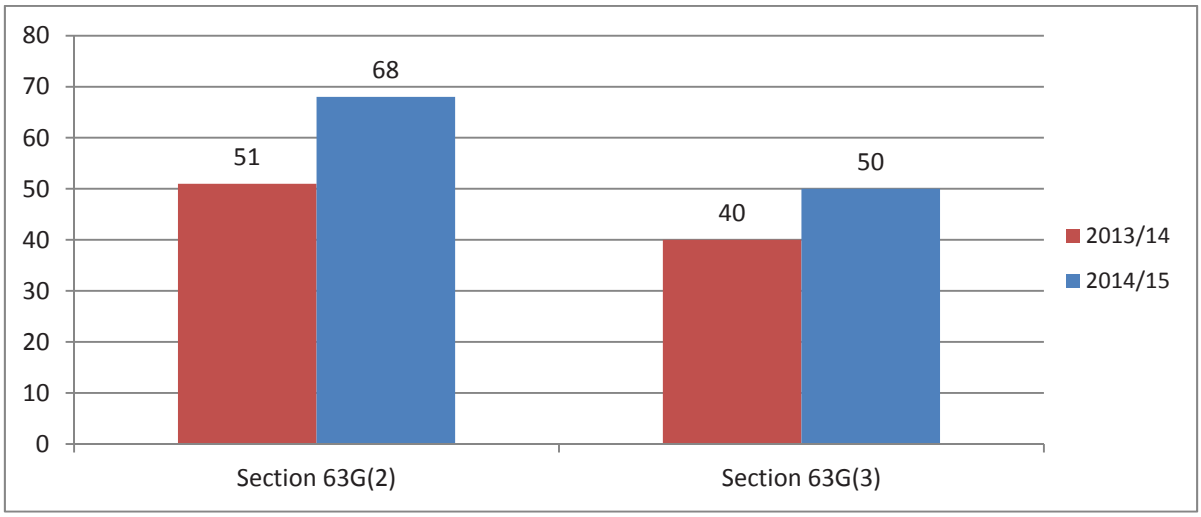
APPLICATIONS: STATISTICAL ANALYSIS

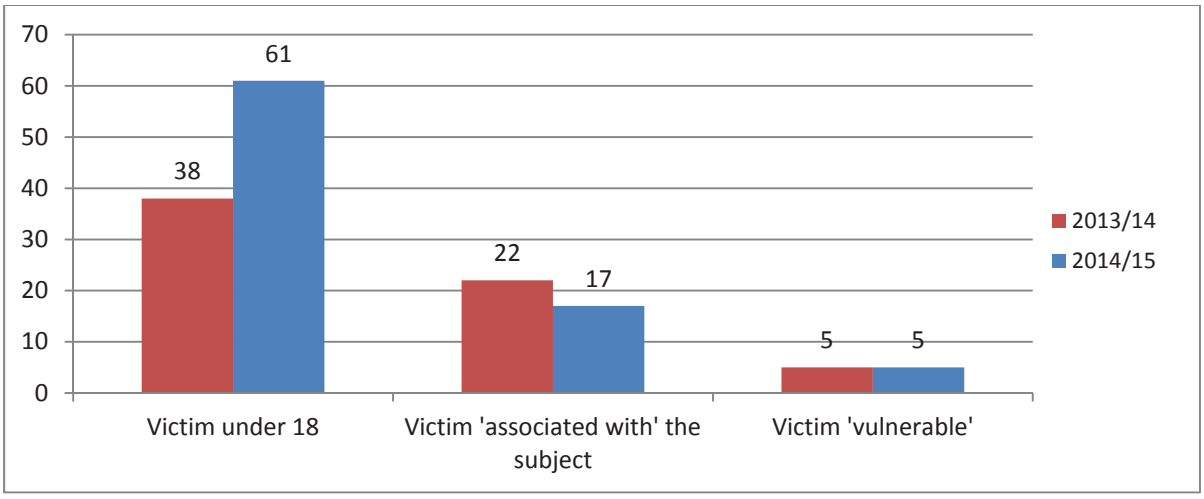
35. The following are features of the 209 applications made between 31 October 2013 and 31 August 2015. References to '2013/14' relate to the period 31 October 2013 to 31 August 2014. References to '2014/15' relate to the period 1 September 2014 to 31 August 2015.

STATUTORY BASIS FOR APPLICATIONS

36. Between 31 October 2013 and 31 August 2015, 119 applications were made under section 63G(2) and 90 were made under section 63G(3).[24] In a number of the former applications more than one of the 'victim criteria' were satisfied; overall, however:

- in 99 of the applications under section 63G(2) the alleged victim was under 18 years of age;
- in 39 the alleged victim was 'associated with' the subject of the application; and
- in 10 the alleged victim was 'vulnerable'.

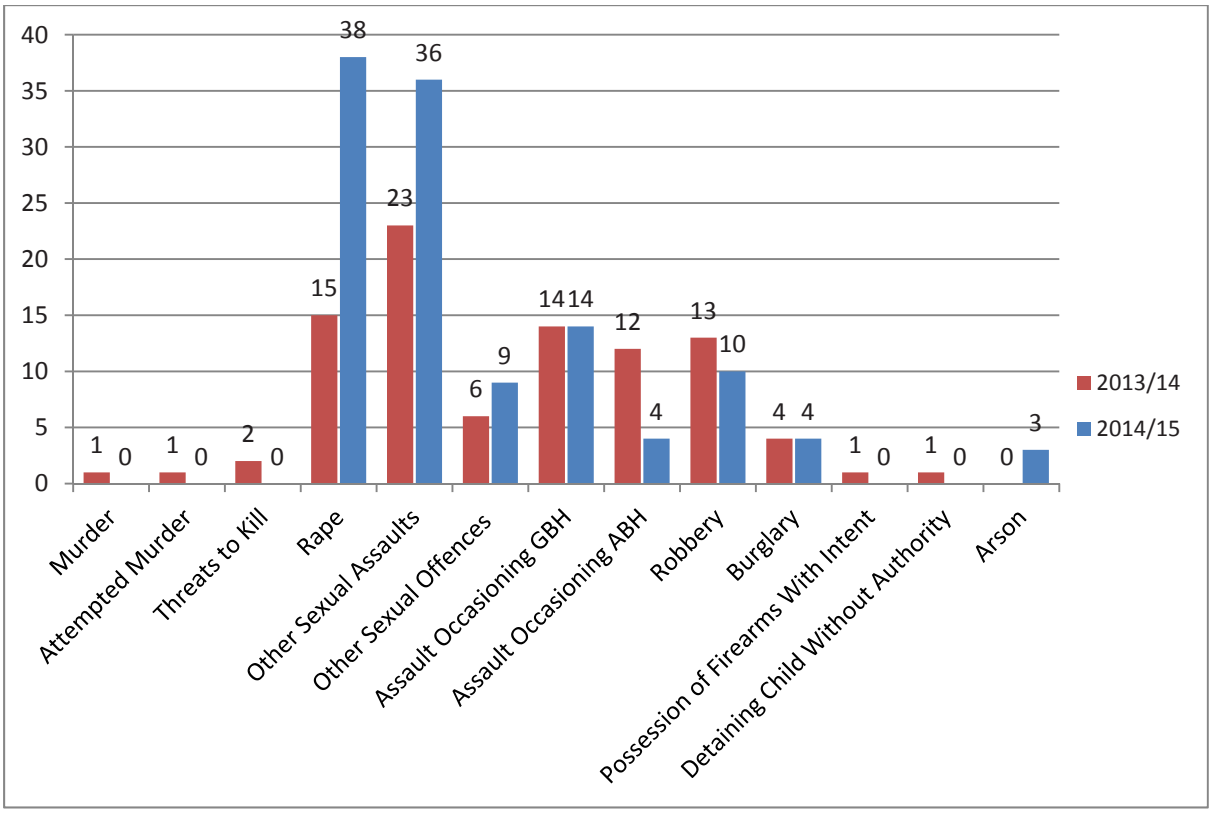




[24] In a few application forms the wrong provision was referred to and/or it was unclear which provision was being relied on. In all cases where the section 63G(2) 'victim criteria' were apparently satisfied, my Office has treated the application as if it were being made under that provision.

QUALIFYING OFFENCES

37. The qualifying offences for which the subjects of those 209 applications were arrested were as follows.

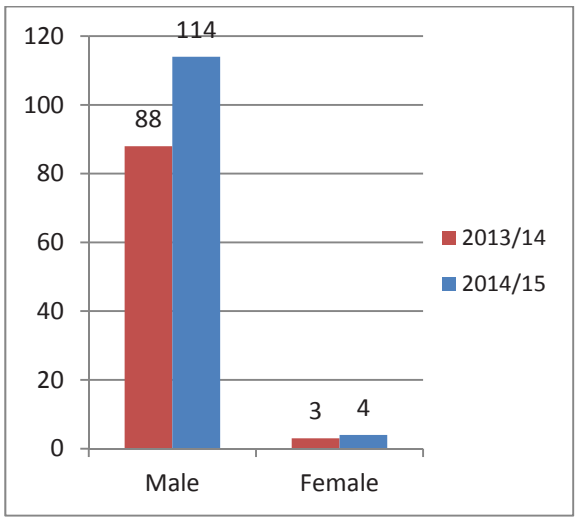


[Note that for two subjects applications were made in respect of more than one qualifying offence. Note also that:

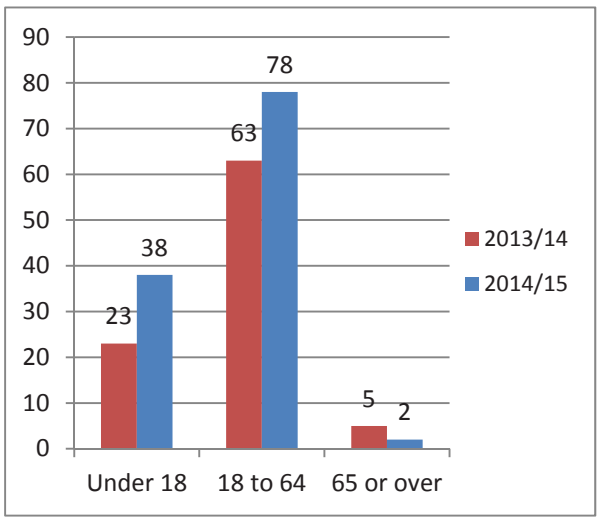
- the figures for 'Rape' include Conspiracy to Rape (×1) and Attempted Rape (×2);
- the figures for 'Robbery' include Conspiracy to Commit Robbery (×2) and Attempted Robbery (×2);
- the 'Other Sexual Offences' in 2013/14 were Indecent Exposure (x4), Voyeurism (x1) and Causing a child to watch/look at an image of sexual activity (x1); and
- the 'Other Sexual Offences' in 2014/15 were Indecent Exposure (x3), Inciting a child under 13 to engage in sexual activity (x2), Possess to show/distribute indecent photo of child (x1), Grooming (x1), Kidnap/Falsely imprison with intent to commit sexual offence (x1) and Causing a child to watch/look at an image of sexual activity (x1).]

SUBJECT CHARACTERISTICS

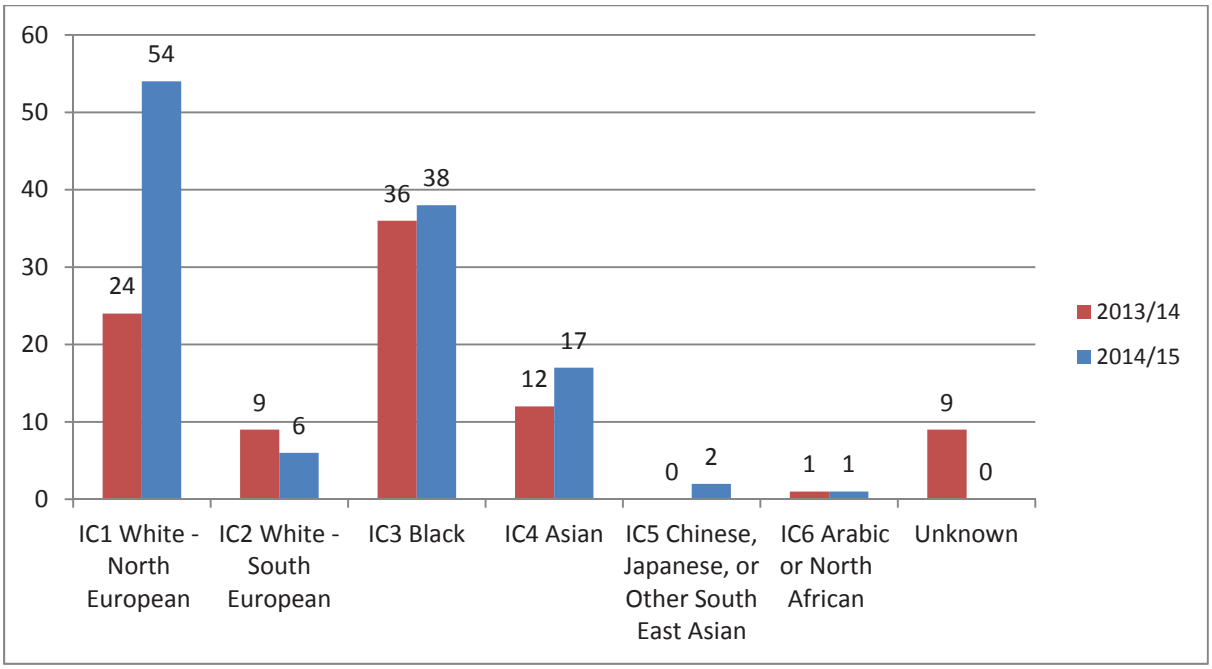
SEX



AGE



ETHNICITY[25]



PREVIOUS ARRESTS ETC.

38. Of the 209 subjects, 156 had previously been arrested and/or had previously had allegations or complaints made against them. Of those 156, 117 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.[26]

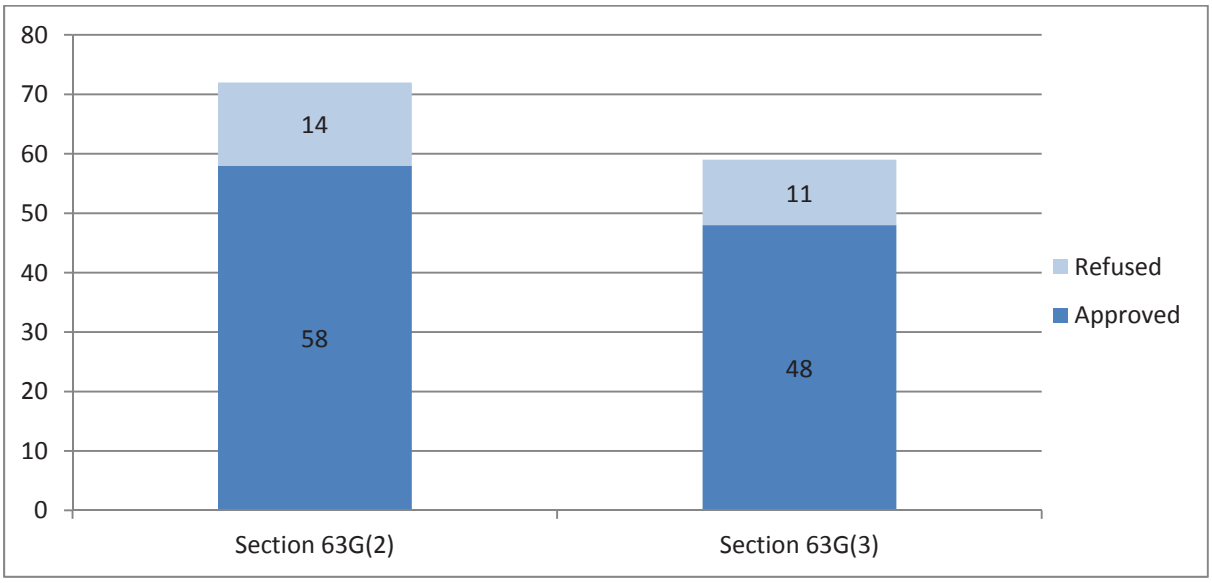
[25] 'Ethnicity' here refers to a police officer's visual assessment of a person's ethnic appearance rather than a subject's self-defined ethnicity. See http://policeauthority.org/metropolitan/publications/briefings/2007/0703/index.html for the code systems used by the Metropolitan Police Service (MPS)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

OUTCOME OF APPLICATIONS: STATISTICAL ANALYSIS

39. Of the 209 applications made by 31 August 2015, 156 had been concluded by that date.[27] Of those 156, 106 had been approved wholly or in part,[28] 25 had been refused, and 25 had been withdrawn. Further information about those concluded applications is set out at paragraphs 60 to 64 below.[29]

STATUTORY BASIS FOR APPLICATIONS

40. Of the 106 applications which had been approved wholly or in part by 31 August 2015, 58 were made under section 63G(2) and 48 under section 63G(3). Of the 25 applications which had been refused by 31 August 2015, 14 were made under section 63G(2) and 11 under section 63G(3).



41. In a number of the decided applications which were made under section 63G(2) more than one of the 'victim criteria' were satisfied. Overall, however:

- in 55 of those applications the alleged victim was under 18 years of age;
- in 25 the alleged victim was 'associated with' the subject of the application; and

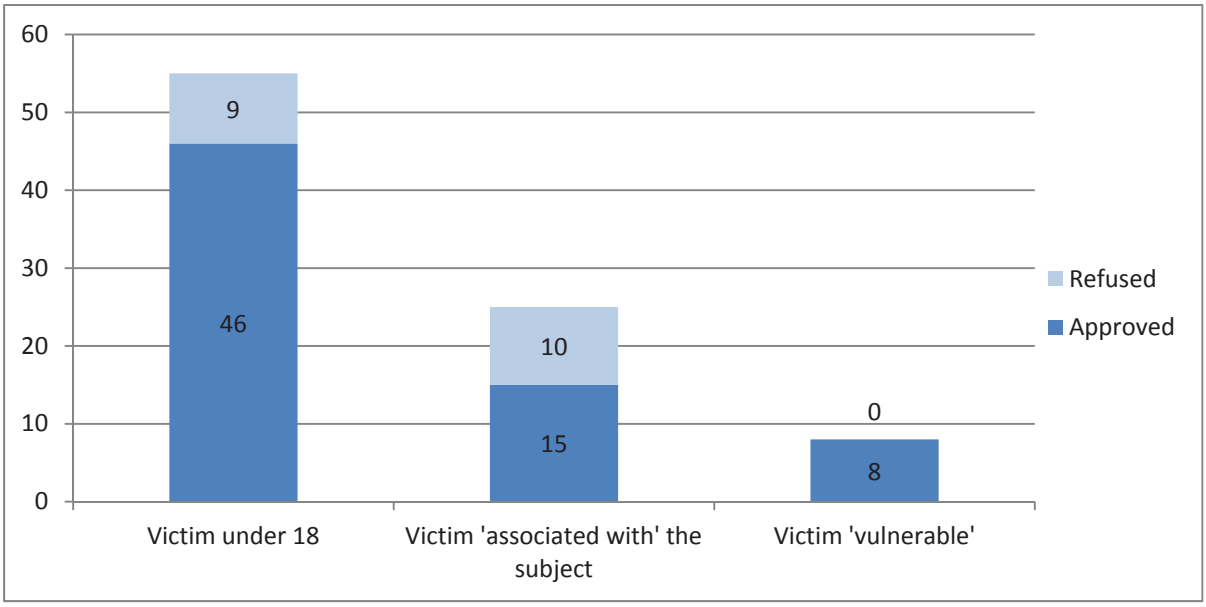
[26] 77 of the 91 subjects of the applications made by 31 August 2014 had previously been arrested and 64 had been arrested on 2 or more previous occasions. 79 of the 118 subjects of the applications made between 1 September of 2014 and 31 August 2015 had previously been arrested and 53 had been arrested on 2 or more previous occasions.

[27] 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.

[28] In one case the retention of fingerprints was approved but the retention of a DNA profile was refused as that profile was being held unlawfully by the applying force. Further information about that case appears at paragraphs 63-64 below.

[29] Of the 91 applications that had been made by 31 August 2014, 40 had been concluded by that date, 25 had been approved, 5 refused and 10 withdrawn. Further information about those 40 applications can be found at paragraphs 51-58 of my 2014 Report.

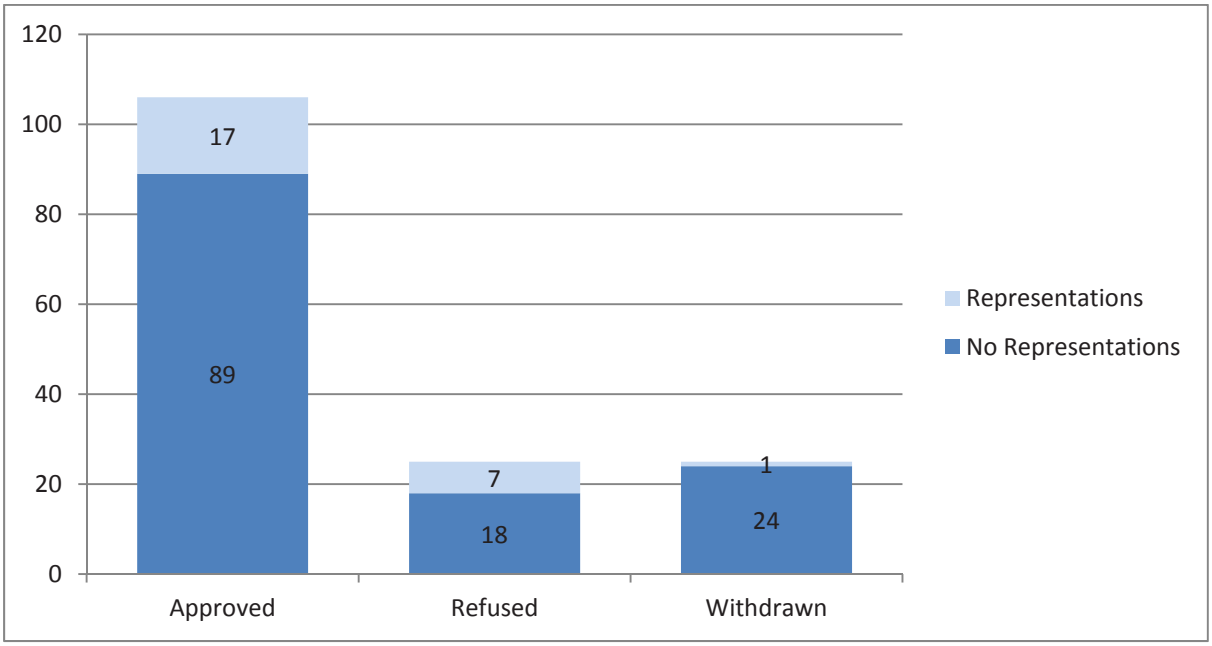
- in 8 the alleged victim was 'vulnerable'.



REPRESENTATIONS

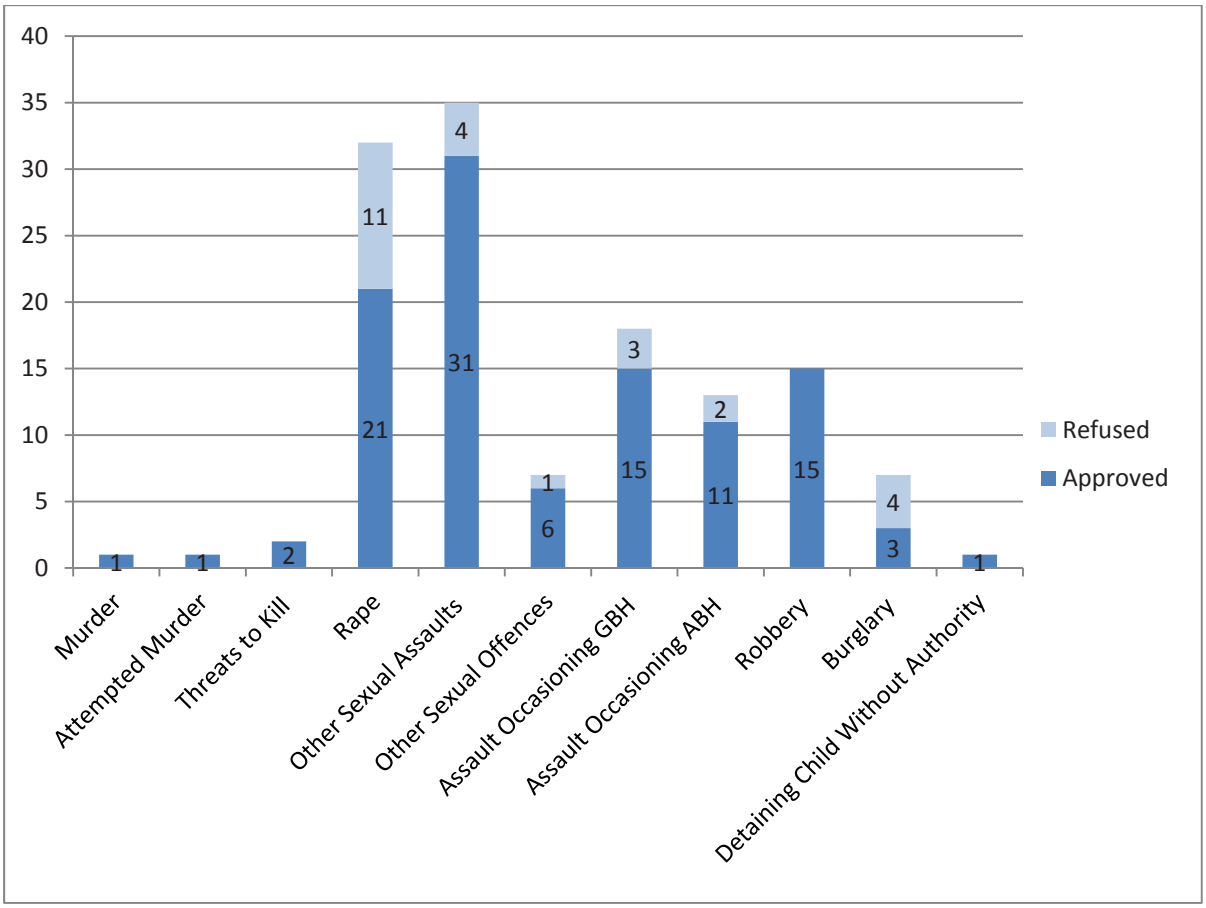
42. In 17 (16%) of the 106 applications which had been approved by 31 August 2015, representations were made by or on behalf of the individual affected.

43. In 7 (28%) of the 25 applications which had been refused by 31 August 2015, representations were made by or on behalf of the individual affected. Representations were also made in one case that was subsequently withdrawn by the police.



QUALIFYING OFFENCES

44. The qualifying offences for which the subjects of the 131 decided applications were arrested were as follows.

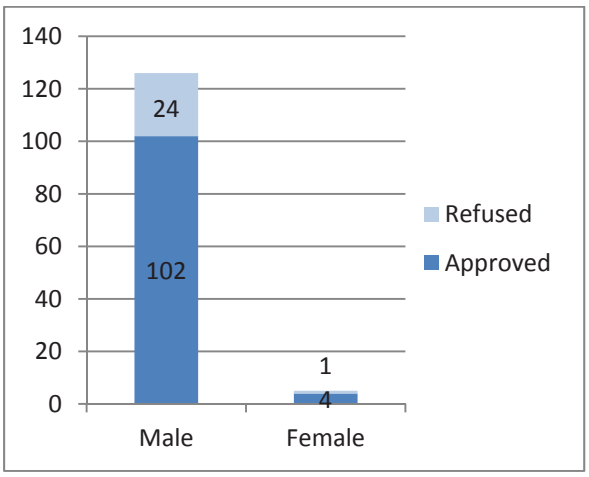


[Note that one of the 131 decided applications was made in respect of two qualifying offences. Note also that:

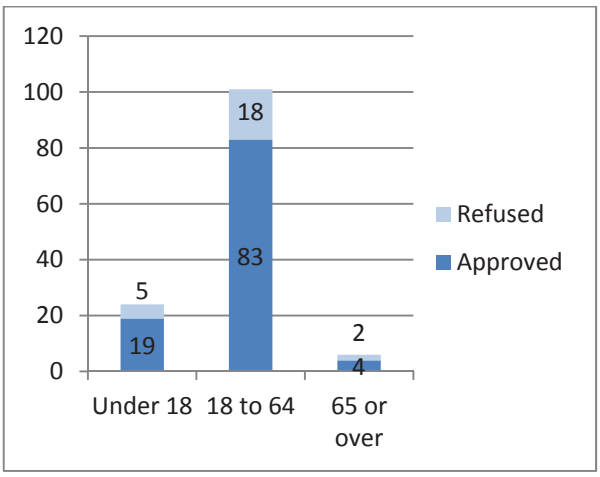
- the figures for 'Rape' include Conspiracy to Rape (×1 approved) and Attempted Rape (×1 approved and ×1 refused).
- the figures for 'Robbery' include Conspiracy to Commit Robbery (×2 approved) and Attempted Robbery (×1 approved).
- the 'Other Sexual Offences' were Indecent Exposure (x2 approved and x1 refused), Possess to show/distribute indecent photo of child (x1 approved), Causing a child to watch/look at an image of sexual activity (x2 approved) and Inciting a child under 13 to engage in sexual activity (x1 approved).

SUBJECT CHARACTERISTICS

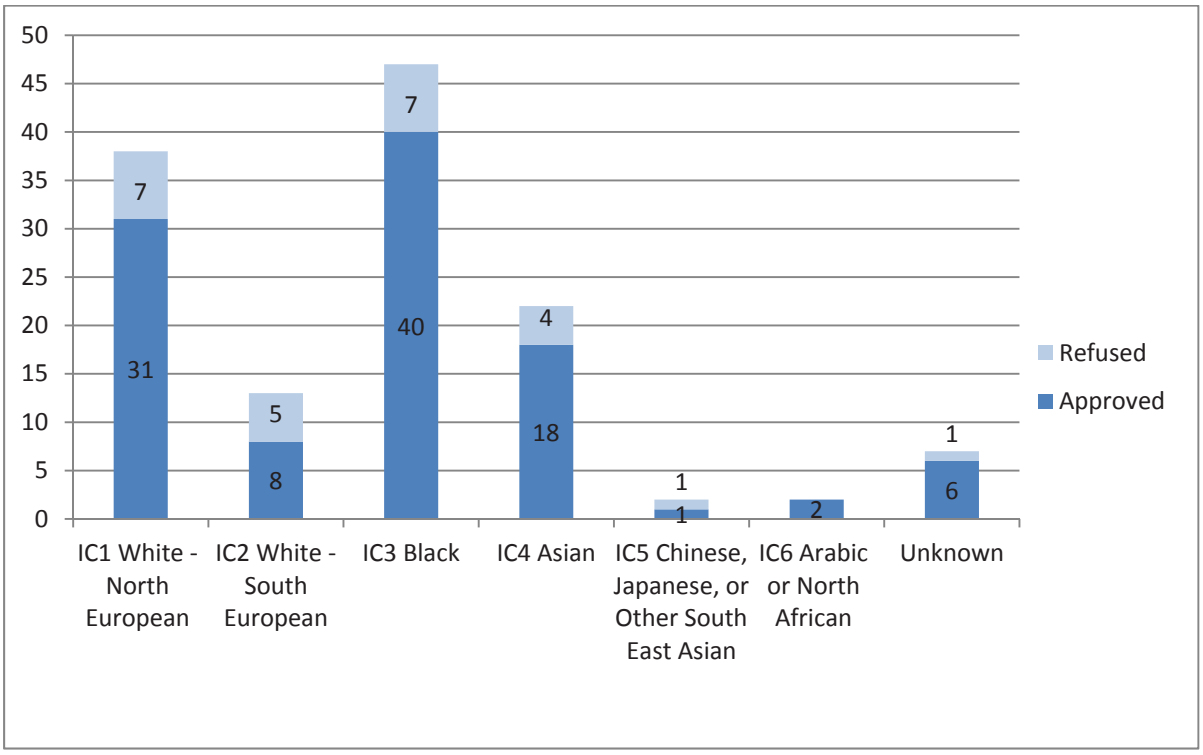
SEX



AGE



ETHNICITY



PREVIOUS ARRESTS ETC.

45. Of the subjects of the 106 applications which had been approved by 31 August 2015, 82 had previously been arrested and/or had previously had allegations or complaints made against them. Of those 82, 65 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.

46. Of the subjects of the 25 applications which had been refused by 31 August 2015, 19 had been previously been arrested and/or had previously had allegations or complaints made against them. Of those 19, 13 had been arrested and/or had been the subject of allegations or complaints on 2 or more previous occasions.

APPLICATIONS WITHDRAWN

47. Of the 25 applications which had been withdrawn by 31 August 2015:

- 1 was withdrawn when it was pointed out that it was ineligible as the relevant arrest had been made before 31 October 2013;
- 1 was withdrawn because the application received by the OBC had not been approved by a chief officer of police: when the application was put before a chief officer, he declined to authorise it;
- 3 were withdrawn when it was discovered that the relevant biometric records had already been deleted because of the force's failure to put an appropriate 'marker' on the PNC;[30]
- 5 were withdrawn when it was discovered that the relevant biometric records had already been deleted by reason of a PNC programming error;[31]
- 13 were withdrawn because the subject was convicted of a recordable offence after the application was submitted (and because their biometric records could therefore be retained indefinitely);
- 1 was withdrawn because the subject was charged with a qualifying offence after the application was submitted (and because their biometric records could therefore be retained for three years); and
- 1 was withdrawn because the applying force thought that the subject had been charged with a qualifying offence after the application was submitted: it subsequently transpired that the subject had not been charged and a new application was made.

[30] These applications were made in respect of allegations of sexual assault against a female, rape and inciting a child under 13 to engage in sexual activity. Further information about such markers appears at paragraph 28 above and paragraphs 244-245 below.

[31] These applications were made in respect of allegations of rape, inciting a child to perform a sexual act, indecent exposure, voyeurism and ABH. Further information about 'erroneous deletions' from the PNC appears at paragraph 221 below.

PRELIMINARY APPLICATIONS, INTERIM NOTIFICATIONS AND ONGOING COMPLEX INVESTIGATIONS

PRELIMINARY APPLICATIONS AND DISCLOSURE

48. 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.

49. Contrary to my expectations, concerns about disclosure have arisen only relatively rarely and in the period to 31 August 2015 only 3 Preliminary Applications were made. Those Preliminary Applications have all gone on to become 'full' applications. It is noteworthy that since April of 2015 the MPS has adopted a process whereby, rather than attaching to the Notification Letter a document which summarises the contents of the relevant BC1 Application Form, it simply encloses a copy of the Application Form in its entirety. Provided only that care is taken to omit or redact unnecessary personal information (such as the names and addresses of victims and witnesses), this time-saving approach appears to be both a sensible and practical one in virtually every case.

50. In a small number of cases I have formed the view that, because of the limited disclosure that had been made to the subject by the applying force, it would be inappropriate for me to attach any weight to a point or points raised in the application form. In none of those cases, however, would my decision have been different if proper information had been provided to the subject. On a few other occasions my Office has alerted applying forces to significant omissions from their Notification Letters and those forces have then chosen to send revised notification letters to the subjects concerned.

51. Finally as regards disclosure I should mention that in a number of cases an applying force has disclosed information to a subject which, on the face of things, it should not have done. This situation has in particular arisen where reference has been made in a Notification Letter to a previous allegation against the subject by a third party in circumstances where that third party had made it clear that they did not want that allegation to be passed on to the subject and/or had told the police about the alleged matter simply so that the police should be 'aware' of it. In cases where such a situation has arisen, my Office has expressly drawn it to the attention of the force concerned.

INTERIM NOTIFICATIONS

52. A significant number of cases about which my Office has been approached have involved subjects who have not been charged with the qualifying offences for which they were arrested but who have been charged with lesser 'non-qualifying' offences relating to the

same incidents (e.g. they have been arrested for Assault Occasioning ABH but have been charged only with Battery).

53. In the early months of 2014 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.

54. As was explained in my previous Report, I concluded 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 NFA the qualifying offence, I will generally be content to accept a later section 63G application 'out of time'.[32]

55. Forces have been asked to inform me of any Interim Notifications which they have given 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 2015 my Office was informed of 76 Interim Notifications, all but one of them by the MPS. As at that latter date, 10 of those Notifications had been followed by applications under section 63G and 55 had 'lapsed' either because (in 45 cases) the individuals in question had been convicted of recordable offences and their biometric records had therefore become subject to indefinite retention or because (in 10 cases) it was decided not to proceed to a full application.

ONGOING COMPLEX INVESTIGATIONS

56. At paragraphs 67-69 of my previous Report I referred to a case involving a long-running investigation in which, although arrestees had been NFA'd:

- that investigation remained ongoing and those individuals remained suspects for the offence at issue;

[32] See paragraphs 61-66 of my 2014 Report. This 'Interim Notification' process is now also used in circumstances where the subject of an application has been arrested for, or charged with, an unrelated offence while the investigation into the qualifying offence at issue was ongoing.

- I was satisfied that the continued retention of their biometric records would be justifiable according to both the letter and the spirit of the PoFA regime; and
- I agreed that the police should place a 'UZ' (or 'Biometrics Commissioner') marker on the PNC in respect of each of those individuals so as to prevent the automatic deletion of their biometric records.

Further problems relating to protracted investigations have now come to light and those problems are addressed in detail at paragraphs 240-243 below. So far as concerns the particular case to which I referred in my previous Report, the relevant investigation is still proceeding and I remain of the view that the continued retention of the records at issue is both lawful and appropriate.

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

57. 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.

58. 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.

59. In the event only 6 such applications had been made to District Judges by 31 August 2015 and all of them were made by the MPS between 31 October 2013 and 31 August 2014. All of those applications were successful and in each of them the District Judge gave detailed reasons for his or her decision.

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

2.3 ISSUES ARISING FROM APPLICATIONS MADE

GENERALLY

60. At paragraphs 73-88 of my previous Report I addressed various issues which had had a bearing on the decisions which I had made on applications under section 63G. In particular, I explained some of my thinking as regards:

- the circumstances in which there will be compelling reasons to believe not merely that DNA and/or fingerprint evidence may be of value in the context of some future investigation or prosecution but also – and importantly – that some useful purpose will be served by the retention of the biometric material at issue in an application;
- the difficulties which arise where applications are made in the context of alleged and/or feared offences of 'domestic violence';
- the importance of the strength or otherwise of the grounds for suspecting that the subject of an application committed the alleged qualifying offence for which he or she was arrested;
- cases involving subjects who suffer from mental health problems or who are in some other way 'vulnerable'; and
- the possible deterrent effect of extended retention.

My thinking as regards those matters has remained largely unchanged and has played a significant part in a number of the decisions that I have made since then.

61. The applications in relation to which those decisions have been made have continued to be founded upon arrests for a wide range of alleged qualifying offences, primarily of a serious sexual or violent nature. Those alleged offences have in particular included:

- a number involving the alleged 'grooming' of children, alleged sexual abuse of a 'familial' and/or 'historic' nature, and alleged sexual offending against individuals who were unusually vulnerable by reason of their age, their consumption of alcohol and/or their mental health issues; and
- others involving alleged street robberies or assaults in which a number of offenders were said to have been involved.

One (which I rejected) related to an individual who had died some seven months before the relevant application was made.

62. Although I have rejected approximately one in five of the applications which I have decided – and although some of them have seemed to me to be markedly stronger than others – I am satisfied that careful consideration was given to each of them by the applying force. Although, moreover, a few of those applications have seemed to me surprising ones to make – usually because of the weakness of the grounds for suspecting that the subject

committed the qualifying offence at issue – none of them has seemed to me obviously unreasonable and misconceived.

63. In one unusual case I approved the extended retention of a subject's fingerprints but not the retention of their DNA profile. In that case the force involved had failed to take a DNA sample from the subject at the time of their arrest for the qualifying offence at issue and was seeking to retain a DNA profile which had been generated following an earlier arrest of that individual in 2011. That profile should in fact have been deleted from the database by the time that PoFA came into effect in October of 2013 and was therefore being held unlawfully by the applying force. After considering detailed representations from the force, I concluded that I could not properly grant the application insofar as it related to the unlawfully held DNA profile and that, even if I could do so as a matter of law, it would not be 'appropriate' for that profile to be retained in the circumstances which had arisen.

64. An important feature of that application – and one which added to the difficulty of deciding it – was:

- that the wrongful retention of the profile had arisen as a result of what the force described as *"a national technical anomaly with PNC"* rather than as a result of a deliberate decision; and
- that if the force had realised at the time of the later arrest that the earlier profile was being wrongfully retained, it could (and no doubt would) have taken a further DNA sample from the arrestee.

That 'technical anomaly' is one of those to which I referred at paragraphs 221-222 of my 2014 Report and to which I return at paragraphs 227-228 below.

THE LIST OF QUALIFYING OFFENCES

65. 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.

66. At paragraph 90 of my previous Report I observed as follows:

> *"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,[34] 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."

67. In the Government's response to my Report[35] Lord Bates said:

"On the basis of discussions with operational partners we recognise that there are some offences which it would be useful to include within the existing list of qualifying offences, including those identified in your report. Any change to existing provisions will require secondary legislation to bring into force. I have therefore asked my officials to give this matter further consideration with a view to amending the list during the term of the next Parliament."

I have continued to pursue this matter with Home Office officials and I understand that it is currently intended that an appropriate Statutory Instrument will be laid before Parliament in mid-2016. I further understand that it is likely that that Instrument will cover a large number of offences other than those to which I drew particular attention, many of which (e.g. 'child stealing') are or can be very similar in substance to offences which are already qualifying offences.

CONVICTIONS OUTSIDE ENGLAND AND WALES

GENERALLY

68. At paragraphs 91-101 of my 2014 Report:

- I explained that sections 61(6D), 62(2A), 63(3E) and 63J of PACE now allow for the taking and indefinite retention of biometric material from individuals who have been convicted of qualifying offences outside England and Wales; and
- I expressed my concerns about various difficulties that had arisen in connection with the implementation of those provisions.

Those concerns were picked up by various media and other commentators and were noted in the Government's response to my Report.

69. I have continued to keep these matters under careful review. Regrettably, however, no substantive progress appears to have been made in connection with any of them.

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

[35] See https://www.gov.uk/government/news/publication-of-the-governments-response-to-the-biometrics-commissioners-first-annual-report

THE NEED TO RE-TAKE BIOMETRICS

70. In my previous report I observed as follows:

> *"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 currently have no option but to go back to those individuals and to take further samples and fingerprints from them under those sections.*
>
> *94. ... 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."*

71. At a meeting with Home Office officials in February of 2015 it was agreed that, although this problem could only be remedied by way of primary legislation, an appropriate amendment to the existing text of section 63J would be relatively easy to formulate. In the event, however, no such amendment has yet been proposed to Parliament and, although I understand that consideration was given to the possibility of that being done during the 2016/17 Parliamentary session, I have recently been informed that no such proposal will in fact be included in the Government's legislative programme for that year.

72. It is in my view desirable that the legislative change which is required in this connection should be made as soon as is reasonably possible. In parts of England and Wales a substantial proportion of those arrested by the police are foreign nationals[36] and I am aware of at least one case in which a force:

- wanted to retain the biometric material of an EU national with relevant foreign convictions who it had arrested and NFA'd; and
- could have done so provided only that it had taken a further DNA sample and set of fingerprints from him; but
- chose not to pursue that option, apparently because of the time and other resources that would have had to be expended on such an exercise.

[36] In the MPS area the figure is approximately 30%: see page 10 of the '*Prüm Business and Implementation Case'* which is referred to at paragraphs 315-318 below.

SCOTTISH AND NORTHERN IRISH CONVICTIONS

73. Although in my previous Report I dealt mainly with problems which have arisen as regards foreign nationals who have been arrested in England and Wales, I noted that difficulties have also arisen in connection with the taking and/or retention of biometric material from UK nationals who have never been convicted in England and Wales but who have been convicted of qualifying offences in Scotland or Northern Ireland.[37] In particular, I noted that:

> "*issues associated with the operation of the PNC may make it impossible for forces in England and Wales to procure the loading and retention of DNA profiles from such individuals pursuant to section 63J*."

It is my understanding that those technical/procedural issues continue to preclude the loading and retention of DNA profiles from such individuals by forces in England and Wales.

74. At paragraph 101 of my previous Report I also observed that it was my understanding:

> "*that consideration [was] already being given to the possibility of seeking legislative changes ... 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)*."

That possibility seemed to me well worth exploring since, whatever may be the position as regards foreign convictions, it is perhaps surprising that the retention regime that applies to those who have been convicted of offences in England and Wales is different from that which applies to those who have been convicted of offences in Scotland or Northern Ireland.

75. Once again no substantive progress appears to have been made in this connection and, once again, I have recently been informed that no changes of the type referred to above will be included in the Government's legislative programme for 2016/17.

LOADING NON-UK CONVICTIONS TO THE PNC

76. Unless and until a non-UK conviction has been recorded on the PNC it is impossible to load to the national databases any DNA profile or fingerprints which have been taken in reliance on that conviction. That reality is of particular significance in this present context because:

- there are strict limitations on the uses to which the UK can properly put conviction information about (non-UK) EU nationals which it obtains from other EU member states;
- it is only in relatively rare circumstances that the foreign convictions of such EU nationals can properly be recorded on the PNC;
- those circumstances are in effect limited to cases where the recording of those convictions on the PNC is reasonably necessary to prevent "*an immediate and serious threat to public security*"; and

[37] See paragraphs 100-101 of my 2014 Report.

- convictions will only be treated as being of that type if they are for offences that fall within the ambit of a list of serious offences which has been approved by the Home Secretary.[38]

Indeed – and for no obviously compelling reason – it seems that, with few exceptions, even convictions of non-UK nationals *outside* the EU will only be recorded on the PNC if they are for offences that fall within the ambit of that list.[39]

77. In my previous Report I explained that I had very recently been informed that changes had been made to that list of offences but that I was as yet uncertain as to precisely how those changes would take effect or as to the extent to which they would address the problems that had arisen.[40] What quickly became clear, however, was that that revised (and significantly expanded) list – which has never been published – leaves scope for the exercise of judgment and/or discretion in a variety of circumstances and that it is desirable that guidance should be issued to ensure that it is applied in a consistent and appropriate manner.

78. Although at a meeting with Home Office officials and others in February of 2015 it was agreed that such guidance should be produced – and, indeed, that it would seem sensible to abandon the existing policy of applying the list to foreign convictions outside the EU as well as to those inside it – neither of those steps has yet been taken. I understand, however, that it is likely that relevant guidance will be finalised within the next few weeks and possible that a revised policy will be adopted within that period. I also understand that, whatever may be the position as regards the amended list itself, it is intended that that guidance will be published.

UK NATIONALS WHO HAVE OFFENDED ABROAD

79. When UK citizens are convicted of offences abroad it is common for their convictions to be notified to the relevant UK authorities and for those convictions then to be recorded on the PNC.[41] No 'loading' difficulties arise as regards such convictions and they are almost always recorded on the PNC whether or not they fall within the ambit of the list that is referred to above.[42] DNA information is rarely (if ever) received in connection with such convictions

[38] See e.g. paragraphs 95-99 of my 2014 Report.

[39] The exceptions are convictions in countries with which the UK has appropriate bilateral 'Information Sharing Agreements' i.e. Albania, Anguilla, Bermuda, Cayman Islands, Ghana, Indonesia, Jamaica, Montserrat, Trinidad & Tobago, Turks & Caicos Islands, the UAE and Vietnam.

[40] See paragraph 99 of my 2014 Report.

[41] See paragraph 283 of my 2014 Report. Whereas when UK citizens are convicted of offences in EU countries there is a legal requirement for those countries to notify the UK of those convictions, there is no such legal requirement for non-EU countries.

[42] Convictions may, however, only be loaded to the PNC in respect of offences where there is an equivalent recordable offence in the UK.

but fingerprints sometimes are. In those circumstances the fingerprints will be loaded to, and retained on, IDENT1.[43]

80. Sections 61(6D), 62(2A), 63(3E) and 63J of PACE apply to any individuals who have been convicted of qualifying offences outside England and Wales and it follows that forces could, if they wished, use their powers under those sections to take and retain DNA (and, if necessary, fingerprints) from UK nationals who have offended abroad but who have never been convicted in the UK. I have no information as to whether – and, if so, to what extent – those powers have in fact been utilised.

CONCLUSIONS

81. In my previous Report I observed that it had been suggested to me that, for the reasons there explained, *"sections 61(6D), 62(2A), 63(3E) and 63J have proved to be of significantly less practical value than might reasonably have been expected."* Although I have been unable to establish how often – if at all – those sections have in fact been utilised, that remains my perception.[44]

82. I of course recognise that it is important that careful thought be given to the desirability and wording of possible amendments to a statutory regime and that such amendments can rarely be made quickly. I also recognise that even changes to non-statutory processes should be carefully thought through. Even so, however, I am concerned that, as yet, little of substance seems to have been done to address the problems which have been identified in relation to the taking and retention of biometric material from individuals who have been convicted of offences outside England and Wales. I will continue to keep those problems under careful review.

83. It is right that I should expressly acknowledge:

- that over the past year or so there has been a substantial increase in the frequency with which police forces, when arresting foreign nationals, check their immigration status and whether they have a criminal record overseas;[45] and
- that over that period the number of foreign convictions of non-UK nationals that have been recorded on the PNC has risen substantially;[46] and

[43] See also in this connection paragraphs 286-289 below.

[44] From the enquiries which I have made of the Home Office and others it appears that no relevant central records are kept.

[45] A directive from the Home Office issued in late 2014 indicated that police forces should submit foreign conviction checks for at least 60% of all EU national offenders by 1 April 2015. Police Forces are now making concerted efforts to increase submission rates with a number of forces, including the Metropolitan Police Service, striving for a 100% compliance rate. [I have been told that these factors could result in ACRO processing approximately 150,000 requests per year.] The Directive was issued in response to a recommendation in the House of Commons Committee of Public Accounts Report of 12 January 2015 (at paragraph 3).
http://www.publications.parliament.uk/pa/cm201415/cmselect/cmpubacc/708/708.pdf

- that the practical significance of the problems referred to above – and the risks to which they give rise – will no doubt diminish as and when the United Kingdom implements the Prüm mechanism (which allows for the automated cross-searching of DNA profiles and fingerprints among EU member states).[47]

However, whilst those developments are clearly to be welcomed, it remains the case that biometric material from people who have been convicted of offences outside England and Wales, which should on the face of things be being retained on the national databases, is in fact being lost.

COMMUNICATING WITH SUBJECTS

MINORS AND VULNERABLE ADULTS

84. I am conscious that, particularly where the subjects of applications under section 63G are minors or vulnerable adults, notification letters from forces and decision letters from me may be alarming to receive and/or difficult to understand. I am also conscious, however, that although it might seem sensible for those letters to be addressed to the parents or guardians of those subjects, they usually include information of a sensitive nature and that those subjects are, as a general rule, entitled to have their right to privacy respected and to choose whether or not to involve their parents or guardians in the matter.

85. In the light of discussions about these issues with representatives of the Information Commissioner's Office the policy which is usually adopted by my Office is to address correspondence only to the subject of an application unless and until they expressly authorise us to do otherwise. Where, however, there is reason to suspect that a subject is a minor or a vulnerable adult, I will normally start my decision letter with wording to the following effect.

> "*In order to protect your privacy I have not sent a copy of this letter to your parent(s) or legal guardian(s). You may think, however, that it would be sensible to seek their help and advice about it*."

I understand that the MPS now adopts a similar approach in the Notification Letters which it sends to such subjects.

86. I remain concerned about this issue and in October of 2015 my Head of Office met with representatives of the ICO and of ACRO[48] to discuss it. At that meeting they considered possible ways of reconciling the obvious desirability of ensuring that a child is properly safeguarded throughout the criminal justice process – including in the context of applications for biometric retention – with appropriate respect for his or her right to data

[46] Between November of 2013 and November of 2014 approximately 950 such convictions were recorded on the PNC. In the following year the figure was about 3,050.

[47] Parliament's recent decision in that connection is addressed at paragraphs 315-318 below.

[48] (i.e. the Association of Chief Police Officers Criminal Records Office)

privacy. I understand that work is continuing in that connection with a view to producing options for discussion by the National Police Chiefs' Council (NPCC).

CONFIDENTIALITY

87. As is mentioned above, notification letters from forces and decision letters from me usually contain information of a sensitive nature which it is important to keep confidential. In particular, they usually contain information about the alleged offence which might well prove embarrassing (or worse) for subjects if it were to come to the attention of third parties. Moreover, in cases where I approve applications I often point out that one of the factors that I have taken into account when arriving at my decision has been that, unless the subject chooses to give further publicity to the matter, any extended retention of their biometric material will be known only to them, to the law enforcement authorities and to me/my Office.

88. In those circumstances my Office of course takes care to ensure that all my decision letters are marked 'Private and Confidential' and that a return address is provided on the back of the envelope for use in the event that delivery to the subject proves impossible. Despite those efforts, however, on at least one occasion a decision letter has gone astray (in that it was undelivered and then 'returned' to a wrong address) and on another occasion a subject – who had denied any criminality but who had chosen not to make representations – expressed great concern and distress about the possibility that the contents of the decision letter and/or of the earlier notification letter might have come to the attention of members of his family.

89. To minimise risks of that sort my Office now sends all decision letters by Recorded Delivery and, if the subject so requests, it notifies him or her before that letter is despatched.[49] Where a subject is untraceable or is known to have left the address provided by the police, a decision letter is not despatched but is instead 'served to file'.

90. One possible way of minimising the risk of sensitive information in decision letters going astray – and/or of unnecessary distress being caused to subjects – would be to adopt a process whereby detailed reasons for approving an application are only provided 'as a matter of course' to subjects who have made representations to me. The submission of representations would be taken as both confirmation of the subject's contact details/preferred mode of contact and as an indication that the subject has a real interest in, and will therefore want to see, full reasons for the decision. In all other cases (i.e. where the subject has made no contact with my Office since the date of the notification letter), a much shorter decision letter would be sent. That letter would simply state that a decision has been made to approve the application and summarise the consequences of that

[49] I understand that the MPS now also sends all notification letters by Recorded Delivery. Other forces have, on occasion, arranged for them to be delivered by way of personal service.

decision. It would, however, also make clear that detailed reasons for the decision will be provided if a request for them is received by my Office by a specified date.

91. It is likely that I will soon adopt a process along these lines. Although in those circumstances a detailed decision letter will not be despatched in every case, a full record of the reasons for each decision will of course be held on the relevant case file so as to be available in the event that they are later asked for by the subject.

RE-SAMPLING

92. On a number of occasions my Office has been contacted about cases in which a force has been minded to make an application under section 63G but has discovered either:

- that no DNA sample was taken at the time of the relevant arrest; or
- that although such a sample was taken, the profile generated from it has by mistake or oversight been deleted from the national database.

In some of those cases the forces concerned have indicated that they intend to ask the subject to consent to the provision of a new sample and then to apply under section 63G for the extended retention of the profile that is derived from it. In almost every case where such a request has actually been made, however, the subject has (perhaps unsurprisingly) declined to provide a further sample and on the only occasion on which the subject agreed to do so, the application was not pursued.

93. On the face of things the police have no power to require an individual who they have arrested to provide a second DNA sample (or indeed a second set of fingerprints) simply because the profile derived from the sample which was taken from that individual when they were first arrested (or the set of fingerprints which was taken from him or her on that occasion) has been deleted from the relevant database in circumstances where it could in fact have been retained. One question which has yet to be resolved, however, is that of what the position would be if a subject in fact agreed to provide such a sample. Although it seems to me most unlikely that the taking of a voluntary sample could provide a practical way of circumventing the retention problems that arise in cases of this type, I have referred that issue to the Home Office for it to consider and, if it thinks it appropriate to do so, to provide relevant guidance to forces.[50]

[50] The issue of re-sampling is also dealt with at paragraphs 240-241 below.

2.4 OTHER ISSUES ARISING AS REGARDS EXTENDED RETENTION

POLICE ENGAGEMENT WITH THE PROCESS

GENERALLY

94. As is pointed out above, by 31 August 2015 police forces had:

- made 209 applications to the Biometrics Commissioner under section 63G;
- given 76 Interim Notifications of possible future applications; and
- made 6 applications to District Judges under section 63F(7).

As is also pointed out above, all but 15 of the applications under section 63G and all but one of the Interim Notifications had been made or given by the MPS.

ENGAGEMENT BY THE MPS

95. From my dealings with the MPS it is apparent that it has engaged fully with the application process under section 63G. 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 2015 it had involved consideration of some 61,000 cases in which individuals had been NFA'd for qualifying offences since 31 October 2013.

96. It is worthy of note that, although I have been told by the MPS that in some 16,500 of those 61,000 'NFA' cases the individuals in question had no previous convictions, by 31 August 2015 the MPS had made applications under section 63G, or had given Interim Notifications, in only 275 of them i.e. in only about 1.6% of those 16,500 cases.[51] It is, however, also worthy of note that although in this current reporting year the MPS has continued to devote substantial time and resources to the making of applications to me under section 63G, it has not pursued the making of applications to District Judges under section 63F(7) (i.e. for extensions to the 'automatic' three-year retention period in respect of individuals who have been charged with, but not convicted of, qualifying offences). I understand that staff changes and resourcing issues have played a significant part in that development and that it is possible that further such applications may be made at a later stage.

[51] It is possible however, that in a significant number of those 16,500 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).

ENGAGEMENT BY OTHER FORCES

97. Whereas only three forces other than the MPS had made applications to me under section 63G by 31 August 2014, by 31 August 2015 five more had done so.[52] Of those eight forces, moreover, four had made more than one such application and one of those four had informed me that, in co-operation with three other forces which had yet to make an application to me, it had established a Biometric Retention Unit similar to that of the MPS. In those circumstances – and in the light of other observations that have been made to me in the course of my visits to forces – it seems clear that there is now a greater level of police engagement with the application process than was hitherto the case.

98. Even so, however, the fact remains that by 31 August 2015 only 15 applications under section 63G had been made to me by forces other than the MPS (i.e. 7% of the total) and that no applications whatsoever had been made by such forces to District Judges under section 63F(7). It remains appropriate, therefore, to consider why applications from forces other than the MPS have remained so relatively scarce.

THE DIFFICULTY OF IDENTIFYING APPROPRIATE CASES

99. Although there are a number of factors which may explain that relative scarcity, it seems possible that one of them has been the difficulty of identifying cases in which such applications might be appropriate and should be considered.

100. In my 2014 Report I pointed out:

- that the limitations of the PNC made it difficult for forces to identify cases in relation to which it might be appropriate for them to make applications for extended retention under section 63G;
- that in the absence of any easy means of identifying such cases, forces who wanted to engage fully with the application process had limited options other than to embark on an elaborate and resource-intensive 'sifting' exercise;
- that a number of forces had indicated to me that they would very much welcome the introduction of a facility into the PNC whereby forces would be able to obtain reports which alerted them to all such cases in their areas ; and
- that although it had been agreed that such a facility would be introduced into the PNC, it was at that time unclear when this would be done.

101. In the event – and apparently because of numerous other pressures on their resources – those responsible for PNC services were unable to introduce such a facility until very recently. I understand, however, that as from 25 November 2015 appropriate 'Daily Reports' have been available to forces.

[52] See footnote 23 above.

102. Whilst the introduction of such a facility will undoubtedly make it easier for forces to identify cases in relation to which applications under section 63G may be appropriate, it is by no means clear that it will lead to a very substantial rise in the number of such applications. Indeed, although it seems:

- that even before its introduction at least three forces other than the MPS had already devised in-house IT 'solutions' which allowed them to identify a significant proportion of such cases; and
- that a significant number of other forces have expressly alerted Investigating Officers to the scope for applications under section 63G and have actively encouraged them to make such applications in appropriate cases,

the number of applications from forces other than the MPS has remained relatively low. Furthermore, I have been informed by more than one such force:

- that they find it difficult or impossible to conceive of circumstances in which it would be sensible for them to make an application; and/or
- that they consider it extremely unlikely that any such application will be made by them even after the introduction of the facility referred to above.

THE BALANCE OF RISK

103. 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.

104. It seems clear that the MPS and a number of other forces have concluded that, in the light of those risks, they should take active steps to identify cases in which applications under section 63G can and should be made. Their views may differ as to the types of cases in relation to which applications may be appropriate – one force has indicated that it only looks actively into cases of a sexual nature – but they all seem to have decided that it is right for them to do more than simply to alert Investigating Officers to the availability of the application process.

It seems equally clear, however, that other forces have taken a different view.

105. At paragraph 113 of my 2014 Report I observed as follows.

> "*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."

106. It is my impression that thinking of this sort remains widespread among forces in England and Wales and that, in the light of it – and although the number of applications that are made to me may rise in the future – it is unlikely (though not of course impossible) that that number will grow very substantially over the next few years. It is certainly the case:

- that, contrary to my expectations at the time of my 2014 Report – and although more forces have now engaged actively with the process – there has been no substantial rise since then in the overall number or rate of such applications; and
- that pressures on police budgets have continued to grow during that period and that those pressures may well grow even further in the future.

THE FUTURE

107. In my 2014 Report[53] I observed:

- that it was at that time impossible to form a reliable view as to the actual or likely practical value of extended retention in the circumstances contemplated by section 63G;[54]
- that it was unlikely that it would be possible to do so before the relevant application process has been in operation for at least 2 or 3 years;
- that it was in my view desirable that that issue be kept under close review and that proper research be conducted into it (and, indeed, into the impact and effectiveness of the new retention regime more generally); and
- that in due course Parliament will no doubt 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 that it will no doubt 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.

In the event – and although I have sought and obtained information about the subsequent arrest history (if any) of each of the individuals in respect of whom applications under section 63G were approved or refused by me between 31 October 2013 and 31 August 2015 – it remains the case that proper research has yet to be conducted in this connection and that none appears to be planned for the near future.

108. Even so – and whilst I remain of the view that it is too early to make a properly informed assessment of the practical value of those statutory processes – the following matters appear to me worthy of particular note.

i. The establishment of a retention regime as regards the biometric material of those who are entitled to be presumed innocent involves, by definition, the striking of a balance between:

- the public interest in the prevention and detection of crime; and
- the individual's right to privacy and/or to be treated otherwise than as a potential suspect.

Absent indefinite retention of every arrestee's biometrics, there will inevitably be times when crimes will go undetected or unprevented because material obtained

[53] (at paragraphs 114-115, 119 and 332-335)

[54] 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).

from individuals who have been arrested but not convicted is not retained for an indefinite period.

ii. Obvious advantages attach to the existence and application of 'bright-line' rules in this context. Such rules are much easier and cheaper to implement than those which afford discretion to police, courts or commissioners. Just such a bright-line rule lies at the heart of the regime introduced by PoFA i.e. that where a person without previous convictions is arrested for, or charged with, a non-qualifying offence, their biometric material will only be retained if they are convicted of that offence. Even as regards qualifying offences, moreover, another bright-line rule underpins the position as regards those who are charged with, but not convicted of, such an offence i.e. that their biometric material may be retained for at least three years.

iii. In its *'Programme for Government'* of May 2010 the Coalition Government which later introduced PoFA indicated that it would *"adopt the protections of the Scottish model for the DNA database"*. The Scottish model adopts a bright-line rule for everyone arrested but not charged i.e. no retention in any circumstances. There is no scope for discretionary retention as contemplated by section 63G. It is true that as regards those charged but not convicted – and similarly to section 63F(7) – the Scottish model does allow not only:

- for automatic retention for three years if arrestees are charged with certain sexual or violent offences (i.e. with offences that are broadly similar to 'qualifying' offences);

but also

- for the police to apply to the Sherriff Court for further discretionary extensions of two years each.

In the event, however, no such applications have, it seems, ever been made.

iv. As I mentioned in my 2014 Report[55] I have been informed that police forces did not ask to be granted a right to make applications for extended retention in the circumstances contemplated by s63G or, indeed, in those contemplated by s63F(7). However, because such a right now exists they, rather than Parliament, largely bear the risks associated with the non-retention of biometric material in those circumstances. In the view of at least some police officers that un-requested transfer of risk is both unwelcome and unfair.

v. If the rate of applications under section 63G and/or section 63F(7) were to rise substantially then, even bearing in mind the new facility on the PNC which is referred to at paragraphs 100-101 above, there would inevitably be a comparable rise in the financial and other resources which would have to be devoted to those applications

[55] (at footnote 47)

by police forces, by courts and by the OBC. There may well be force in the contention that those resources could be better and more productively spent and, indeed, in the contention that there are more cost-effective ways of reducing any risk to the public that might be posed by those in respect of whom such applications could be made.

vi. In the light of:

- the Scottish example;
- the most recent 'match rate' data that is available from the National DNA Database;[56] and
- the relatively small number of applications that seem likely to be made under section 63G or 63F(7),

there would appear to be little reason to fear that the abolition of the section 63G and 63F(7) procedures would significantly imperil public safety or significantly reduce the efficacy of the national databases. Moreover – and whilst it would be much more difficult to reconcile with the general presumption of innocence and/or the proposition that the biometric records of innocent people should be removed from the databases[57] – there would appear to be even less reason to fear that such would be the effect of substituting for the section 63G procedure a 'bright-line' rule whereby the DNA profiles and fingerprints of those arrested for, but not charged with, qualifying offences are retained for (say) 3, 6 or 12 months in every case.

109. I understand that it is likely that PoFA will be subject to at least some form of post-legislative scrutiny in 2016/17. It would seem obviously desirable for that scrutiny to include detailed scrutiny of the effectiveness and proportionality of 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. By that time those processes will have been in operation for some three years and it should be possible for appropriate research to have been conducted in relation to them. In the light of that practical experience and research it will, I hope, then be open to Parliament to make a properly informed decision as to the future of those processes and, in particular, as to whether to maintain, amend or abolish them and/or as to whether to substitute for them some new bright-line rule or rules.

[56] (which indicates that that rate has risen since the introduction of the more restrictive retention regime provided for by PoFA: see section 1.3 of the National DNA Strategy Board's 2014/15 Annual Report at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484938/52921_NPCC_National_DNA_Database_print_ready.pdf.

[57] See e.g. the Written Ministerial Statement that is referred to at paragraph 205 of my 2014 Report.

3. NATIONAL SECURITY DETERMINATIONS AND RELATED MATTERS

3.1 STATUTORY BACKGROUND AND GUIDANCE

STATUTORY BACKGROUND

110. 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').

111. 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.

112. 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'.[58]

113. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[59] 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,[60] 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.

[58] 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.

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

[60] (i.e. that in some cases 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)

114. 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.

115. 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.

116. 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

117. 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.

118. Such Guidance was issued in June of 2013 and a copy of it can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf.

119. As I pointed out in my 2014 Report, the section of that Guidance which deals with DNA samples requires updating to take account of changes introduced by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014.

3.2 THE NSD PROCESS

GENERALLY

120. The NSD process is primarily one for Chief Officers.[61] 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.

121. 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.

122. 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. My Office also receives copies of any applications that are refused by Chief Officers.

123. 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.

[61] 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.

APPLICATIONS FOR NSDs

SUBMITTING APPLICATIONS

124. The process of compiling and submitting applications for NSDs to Chief Officers 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/PSNI and, where appropriate, 'sanitised' so as to take proper account of relevant sensitivities.

125. 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."*[62]

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

126. It is, of course, for Chief Officers to decide what information they require when considering whether to make or renew NSDs. 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*

[62] 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."*

is not retained and the potential benefit that would derive from the extended retention of the biometric material in question."

127. In my 2014 Report[63] I summarised the sort of information and analysis that I had suggested to JFIT and others should be included in applications to Chief Officers for NSDs and I indicated that I had been impressed by the extent to which those suggestions had been adopted in practice. As a general proposition I have continued to be impressed by the fullness of the information and analysis in such applications.

THE MAKING AND RENEWING OF NSDS BY CHIEF OFFICERS

128. 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.

129. 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.

THE COMMISSIONER'S ROLE

130. 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.

131. 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

[63] (at paragraphs 144-146)

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.

132. 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.

133. 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.[64]

134. 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.[65]

135. 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.

[64] Further information is provided in this regard at paragraph 158 below.

[65] 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

136. 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).

137. Until 31 October 2013 – and as has been pointed out 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[66] 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 October of 2015 the Home Secretary agreed to a further extension of that period until 31 October 2016.[67] In practice, then, Legacy Material which cannot otherwise lawfully be retained must be destroyed/deleted by 31 October 2016 unless an NSD is made in respect of it. If an NSD is made in relation to such Legacy Material before 31 October 2016, that material may be retained for the period that that NSD has effect.

[66] 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).

[67] The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) Order 2015 No.1739 (http://www.legislation.gov.uk/uksi/2015/1739/contents/made). [See also in this regard paragraph 162(vii) of my 2014 Report.]

138. 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-terrorism legislation from individuals who have 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 (CTA)	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 (CTA)	S.18 CTA DNA profiles/fingerprints.	3 years
Schedule 6, Paragraph 12 Terrorism Prevention and Investigation Measures Act 2011 (TPIMs Act)	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 (TPIMs Act)	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.

LEGACY MATERIAL

139. 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 2016[68] 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 less far advanced than might have been hoped, substantial progress has been made and I understand that JFIT and PSNI are confident that it will be completed by that date. 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.

140. It is possible that, given the way in which the new regime has been introduced, Legacy Material may lawfully be retained until 31 October 2016 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 (and save only as regards material processed by PSNI) 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.[69]

NEW MATERIAL

141. I am likewise satisfied that, as regards New Material, assessment work is being done properly and with care. Three issues have, however, arisen in relation to the handling of New Material which merit specific mention.[70]

HANDLING DELAYS

142. In my 2014 Report[71] I said that I had recently been informed that, as a result of delays in the handling of New Material and/or in the provision of relevant information to SOFS[72] and JFIT,

[68] (previously 31 October 2015: see paragraph 137 and footnote 67 above)

[69] PSNI has indicated that it will retain all legacy material which is not subject to an NSD until nearly the end of the transitional period (i.e. 31 October 2016).

[70] A further – and important – issue in relation to the retention of such material is addressed at paragraph 168 below.

[71] (at paragraph 161)

it was possible that a small quantity of such material which could and should have been made subject to NSDs before the relevant statutory retention periods expired would in fact have to be deleted. I also said that I would be making urgent enquiries into that matter but understood that steps had already been taken to reduce the risk of any such delays in the future.

143. I am satisfied that such steps had indeed been taken and, moreover, that since that time JFIT has made real efforts to ensure that relevant material and information is quickly forwarded to SOFS/JFIT by other parties to the NSD process. Even so, however, I understand that by 31 October 2015 handling and other delays had led to a situation in which the statutory retention periods in respect of the biometric records of at least some 450 individuals had expired before NSDs could be or had been made in relation to them. Although it seems unlikely that NSDs would have been applied for and made in relation to more than a small proportion of those records, I also understand that in about 10% of those cases it is possible that NSDs would have been applied for. Indeed, in at least 3 of those cases such applications had in fact been made and approved.

144. The full scale and continuing nature of the problems caused by delays in the NSD process have only recently become apparent and I have been assured that further work is being done as a matter of urgency to prevent such problems occurring again and to mitigate their consequences. I am keeping that work – and the issue of delays in the NSD process more generally – under close and active review.

DETERMINATIONS MADE BY OFFICERS OF INSUFFICIENT RANK

145. The applications for 4 of the NSDs submitted to my Office for review by 31 October 2015 had been approved by officers of insufficient rank.[73] Since an NSD 'made' by such an officer can have no lawful effect, those cases were referred back to JFIT for them to take steps to seek the approval of an officer of proper rank or, if appropriate, to destroy the relevant material. In the event it later became apparent that in 3 of those cases the relevant retention periods had already expired and that the biometric material would therefore have to be destroyed/deleted. In the remaining case the application for an NSD will, it seems, be re-submitted for approval by an officer of sufficient rank.

146. It appears that the mistakes that were made in those cases arose out of a misunderstanding by the force concerned of the requirements of the NSD process. I have been informed that those requirements have again been brought to the attention of that force and, indeed, that they will again be brought to the attention of all forces.

[72] Secure Operations – Forensic Services ('SOFS') were previously known as Counter Terrorism Forensic Services ('CTFS') and are responsible for the CT databases.

[73] (i.e. by either a Detective Chief Inspector or a Chief Superintendent)

147. Section 63M of PACE[74] allows for biometric material which is taken in connection with an arrest under that Act to be *"retained for as long as a national security determination made by the Chief Officer has effect in relation to it"*. Notwithstanding that provision, however, it remains the case that – as is explained at paragraphs 25-27 above – once a decision has been made to take 'no further action' against an arrested individual who has no previous convictions, the biometric material taken in connection with his or her arrest will usually fall to be destroyed/deleted within a matter of days.

148. In May of 2015 JFIT raised with me concerns about the possibility that biometric material that has been obtained from an arrestee in the context of a terrorism-related investigation – and that should be retained pursuant to an NSD – will in fact be lost because it will be impossible to arrange for an NSD to be made in the time available. In particular, JFIT's concern was that such a situation might arise in circumstances where the individual in question has been arrested otherwise than under section 41 of TACT and is thereafter quite quickly NFA'd.[75] It is by no means uncommon for such arrests to be made in the context of terrorism-related investigations.

149. Although statistical analysis suggested that a problem of this type was likely to arise in only a relatively small number of cases, it was obviously important that steps be taken to minimise the risk that biometric material of possible CT significance might be deleted 'prematurely'. In that connection it was noted:

    i. that in the context of any terrorism-related investigation it is likely that, before any decision is made to NFA an arrestee, significant research will have been carried out into that arrestee and into his/her associates; and

    ii. that, whilst the relevant legislation provides that NSDs can be made *"for a maximum of 2 years"*, it prescribes no minimum duration for them.

150. Against that background – and put shortly – it was agreed that JFIT would develop a process whereby it could quickly seek and obtain an 'emergency' or 'holding' NSD which would ensure that biometric material of possible CT significance is not lost by reason only of the fact that there is insufficient time to complete the normal NSD process before the expiry of the relevant retention period. Such an NSD would last only for a limited period – say 4 months – and its purpose (which would be made clear to the relevant Chief Officer) would be to allow time for a proper assessment of the individual's activities and associations and, if appropriate, for a 'full' NSD application to be made. It would then be for the Chief Officer to decide whether or not to make such an NSD.

[74] (as introduced by section 9 of PoFA)

[75] As is apparent from the schedule at paragraph 138 above, biometric material that is taken from individuals who are detained under s 41 of TACT may be retained for 3 years even if the arrestee has no previous convictions and is NFA'd within that period.

151. I understand that JFIT are taking steps to develop such a process and that PSNI may also do so. As I have informed them, I will expect my Office to be notified of any such application – and of the making of any 'emergency' or 'holding' NSD – at the earliest possible opportunity.

NUMBERS

152. In my 2014 Report[76] I observed that it had 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 were at that time being held by the police or other law enforcement authorities for national security purposes; or
- the number of NSDs that had been made or the number that I had reviewed.

I also observed that I was not wholly persuaded that either of those suggestions was correct – or that, if they were, that that would inevitably remain the case in future years – and that I would keep that issue under close review.

153. This year I have sought and obtained agreement to disclose the following statistical information, the bulk of which has been provided to me by SOFS and/or JFIT.

POLICE HOLDINGS ON THE CT DATABASES

154. At the commencement of the 'biometric' provisions of PoFA on 31 October 2013 the DNA profiles and/or fingerprints of some 6500 identified individuals were being held by police forces on the national CT databases. The comparable figure as at 31 October 2015 was some 7800. That latter figure encompasses both new additions to the databases since 31 October 2013 and deletions from those databases after that date.

155. Of the individuals whose biometric records were being held by the police on those databases as at 31 October 2013 some 3800 (i.e. about 60%) had never been convicted of a recordable offence (and, absent appropriate NSDs, their biometric records would therefore have fallen to be destroyed/deleted after the expiry of the 'transitional' period). The comparable figure as at 31 October 2015 was some 4350 (i.e. about 55%).[77]

[76] (at paragraph 162)

[77] Once again that latter figure encompasses both new additions to the databases since 31 October 2013 and deletions from those databases after that date.

CASES REVIEWED AND NSD APPLICATIONS MADE

156. By 31 October 2015 the cases of approximately 1900 individuals who had never been convicted of a recordable offence but whose biometric records were nonetheless being retained on the national CT databases had been reviewed by JFIT/PSNI for NSD purposes. By that date JFIT/PSNI:

- had submitted applications for NSDs to Chief Officers in respect of some 217 (i.e. approximately 11 %) of those individuals; and
- had made final or at least provisional decisions not to submit such applications in respect of the remainder (i.e. approximately 89%) of those individuals.[78]

Approximately 85% of those decisions were made on the grounds that there was insufficient evidence to justify the making of such an application. The remainder were made on other grounds e.g.:

- because the relevant biometric material was Legacy Material and the individual in question had been convicted of an offence since 31 October 2013 (and therefore their biometric records could lawfully be retained even in the absence of an NSD); or
- because the relevant retention periods had already expired.[79]

UPSHOT OF NSD APPLICATIONS

157. Of the 217 applications for NSDs that had been made to Chief Officers by 31 October 2015:

- 113 had been approved by Chief Officers or their deputies;
- 4 had been approved by officers of less senior rank;[80]
- 15 had been declined by Chief Officers or their deputies; and
- 85 had yet to be decided.

I have been assured by JFIT that in all the cases where an application by them for an NSD has been declined, the relevant biometric material has quickly been destroyed/deleted.

158. Of the 117 NSDs that had purportedly been made by 31 October 2015, I had reviewed 94 by that date. Of those reviewed:

- I had 'approved' 73;
- I had 'not approved' one and had made an order for the destruction/deletion of the biometric material covered by it;
- I had referred 3 back to JFIT because the NSDs appeared to have been incorrectly made (in that the relevant retention periods appeared to have expired before the NSDs were made');[81] and

[78] Every final decision not to submit an application for an NSD is made by an officer of at least Superintendent rank.

[79] See e.g. paragraphs 142-144 above.

[80] See paragraphs 145-146 above.

- I was awaiting further information in relation to 17 about which my Office or I had raised queries with JFIT/PSNI.[82]

As is mentioned at paragraphs 131-133 above, it was inevitable that, during at least the early operation of the NSD process, I would quite often require further information about NSDs that were submitted to me for review and/or that I would want to look behind the summarised information on NSD application forms and seek details of the underlying intelligence. In the event my Office or I sought further information from JFIT/PSNI about 39 of the 94 NSDs which we had reviewed by 31 October 2015 and we obtained and considered details of the underlying intelligence in 3 of those cases. We have earmarked a further 10 of those cases for 'dip-sampling' during 2016.

OBSERVATIONS

159. Although a number of factors have contributed to the slow implementation of the NSD process, I am satisfied that those factors have now been addressed and I understand that JFIT and PSNI are confident that all Legacy Material can and will be properly assessed by the expiry of the (extended) transitional period on 31 October 2016. It is clear, however, that procedural errors and handling delays in relation to New Material have given rise to significant difficulties and that those errors and delays have led, or will lead, to the loss of a significant number of biometric records that probably could and should have been retained. I have been assured that urgent work is being done to prevent such errors and delays arising in the future and I am keeping that work – and these matters more generally – under close and active review.

160. In my view JFIT and PSNI have made real efforts to implement the NSD process in a sensible and proper manner and I am grateful to them for their open and helpful approach in their dealings with me.

161. As is suggested by the information set out above, it seems that JFIT/PSNI have been giving careful consideration to the question of whether or not there are good grounds for making applications for NSDs and that Chief Officers and their deputies have been giving careful consideration to those applications before deciding whether or not to approve them.

162. Finally – and as I observed in my 2014 Report – in the context of the establishment and operation 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

[81] See in this connection the last sentence of paragraph 143 above. It was subsequently agreed that the biometric records in those cases fell to be deleted from the CT databases.

[82] Those 17 included the 4 referred to at paragraph 145 above in which the NSDs appeared to have been 'made' by officers of insufficient rank. As is there pointed out, it later became apparent that in 3 of those cases the relevant retention periods had already expired and thus that the relevant biometric records would have to be destroyed/deleted.

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.

THE USE 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.

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

OVERSIGHT FUNCTION

164. 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

165. 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.

166. 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.

167. The CT DNA Database is a standalone database of CT-related DNA profiles and crime scene stains. It is operated solely by SOFS. 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 SOFS. All new DNA profiles and ten-print fingerprint sets which are loaded to the NDNAD and IDENT1 are 'washed through' those CT databases.[83] Insofar as 'Legacy' biometric records on the CT databases fall within the ambit of the PoFA regime I have seen nothing to suggest that they, or that copies of them, are being retained or used otherwise than in accordance with the relevant statutory provisions. The position as regards New Material is, however, much less satisfactory.

168. As is pointed out at paragraphs 142-144 and 159 above it has recently become apparent that, in respect of significant quantities of New Material, the relevant statutory retention periods have expired before NSDs could be or have been made in respect of it. It has also recently become apparent that, despite that fact, some or all of that material has remained on the CT databases. I have been assured that urgent steps are now being taken to procure the speedy deletion of New Material that has remained on the CT databases beyond its lawful retention date and to ensure that similar errors are avoided in the future. These are, of course, again matters which I am keeping under close and active review.

169. 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.

170. I mentioned in my 2014 Report 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.[84] I also observed that the relevant stakeholders recognised that it was important that proper governance arrangements and documentation be put in place as quickly as possible. Although some limited progress has been made in that connection, much remains to be done. Whilst I recognise that other and more pressing matters have understandably taken precedence, I consider this 'governance deficit' to be unfortunate and I shall continue to press key stakeholders about it.

[83] Further information about the cross-searching of those databases was set out at paragraphs 170-174 of my 2014 Report.

[84] 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

4. THE DESTRUCTION AND/OR DELETION OF BIOMETRIC MATERIAL

4.1 DNA SAMPLES

BACKGROUND

171. 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.[85] That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.

172. 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 continued to take a particular interest in the implementation of the PoFA 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.

173. 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 an order to that effect is made by a District Judge.[86] 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[87] was that DNA samples were specifically excluded from the 'CPIA exception' that applied as regards DNA profiles and fingerprints.

174. Various 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 samples and

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

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

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

provisions which were broadly (though not entirely) to that effect were introduced by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014. While that section was undergoing legislative scrutiny it was acknowledged by the Government that it was important that there be independent oversight of the retention of DNA samples pursuant to that exception and that responsibility for that oversight should lie with the Biometrics Commissioner.[88] I share the view that the retention of DNA samples in this context merits particularly careful attention.[89]

HAVE SAMPLES BEEN APPROPRIATELY DESTROYED?

GENERALLY

175. 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').[90] As I explained in my 2014 Report, I have visited each of those FSPs – one of them on two occasions – and I have found no reason to doubt that, as was claimed by the Government, some 7,753,000 DNA samples were destroyed in anticipation of the commencement of PoFA in October of 2013. I have also found no reason to suspect that since that time (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.

176. The three independent FSPs mentioned above are subject to regular independent assessment and 'auditing' by the United Kingdom Accreditation Service ('UKAS'). In late 2014 it was agreed by the Home Office that, as part of UKAS's work in relation to FSPs, it would 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. Since then UKAS has made 'scoping' visits to each of the FSPs and it has been able to gain at least some level of assurance as regards compliance by those FSPs with key aspects of PoFA including, in particular, the requirements relating to the destruction of DNA samples. My understanding is that nothing of significant concern has been revealed by those visits, that work is now underway to formalise the making of 'PoFA compliance checks' in the context of the current UKAS assessment mechanism, and that it is envisaged that such checks will be conducted during assessment visits by UKAS every other year.

177. Although I had hoped that it would also be possible for UKAS to carry out 'PoFA compliance checks' on police forces, key stakeholders consider that an arrangement along those lines is

[88] See paragraphs 181-182 of my 2014 Report and section 20(6) of PoFA.

[89] Further information about the development of the CPIA exception was provided at paragraphs 178-182 of my 2014 Report.

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

unnecessary and would be disproportionate. I have therefore carried out such checks myself in the course of visits to forces. By the time of my 2014 Report I had made two such visits: one to a single force and one to a forensic 'hub' serving four forces.[91] In this current reporting year I have visited four further forces[92] together with a forensic 'hub' which serves five more.[93] Further information about those visits appears at paragraphs 191-210 below.

178. I have been impressed by the openness which forces have shown me during those visits and by their readiness to share information with me. I have also been struck, however, by the fact that the prospect of a visit by me appears to have acted as a useful spur to at least some of those forces to re-visit the procedures which they have adopted as regards PoFA-related matters – including those relating to the retention and processing of DNA samples – and that in the course of that process various 'gaps' and deficiencies have been identified.

179. I am satisfied that proper steps have been, or are being, taken to remedy those gaps and deficiencies and, more generally, that real efforts have been, and are being, made by the forces I have visited to ensure full compliance with the PoFA regime. I am also satisfied that insofar as DNA samples have been retained 'in force' for longer than they should have been, the numbers involved have been relatively modest, their retention has been a function of oversight rather than design, and the position has either already been remedied or will be remedied in the near future.

180. My ability to carry out effective 'PoFA compliance checks' on forces is inevitably limited and I remain of the view that more could usefully be done in that regard. This is a matter that I intend to pursue with HMIC.

THE CPIA EXCEPTION

GENERALLY

181. It is clearly open to forces to take differing views as to the circumstances in which a DNA sample "*is, or may become, disclosable*" under the CPIA or any relevant code of practice – and it seems equally clear that forces in fact do so. In my 2014 Report I observed that there appeared to be widespread uncertainty as to the circumstances in which the CPIA exception could properly be relied on and I recommended that the Home Office re-visit and expand upon the guidance which it had issued to forces in connection with that exception.[94] In the Government's response to that Report Lord Bates agreed that *"further guidance on this issue ... would be beneficial."*

[91] See paragraphs 193-197 of my 2014 Report.

[92] i.e. Sussex Police, Merseyside Police, Greater Manchester Police and Gwent Police.

[93] i.e. East Midlands Special Operations Unit Forensic Services serving Derbyshire Constabulary, Leicestershire Police, Lincolnshire Police, Northamptonshire Police and Nottinghamshire Police.

[94] See paragraphs 201-202 of my 2014 Report.

182. Although work has been done since that time to clarify and improve relevant passages in the NDNAD Strategy Board's '*Policy for Access and Use of DNA Samples, Profiles and Associated Data*', it remains my view that clearer guidance is required as to the proper application of the CPIA exception. I shall continue to press for such guidance to be produced.

NUMBERS

183. 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 continued to monitor the numbers of such samples that are being retained pursuant to that exception.

184. To assist me in that connection the NDNAD Delivery Unit (the 'NDU') has continued to provide 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'. Helpful though those schedules are – and as I explained in my 2014 Report – they can at best provide me with only an approximate picture of the position as regards the retention of samples pursuant to the CPIA exception.

185. For a number of technical and other reasons the most recent (broadly) reliable retention figures that are available to me relate to the position as at 30 June 2015 and, in the light of those figures, it seems to me likely that as at that date:

- about 27,700 DNA samples were being retained by FSPs and forces pursuant to the CPIA exception (about 2,480 being arrestee samples and about 25,220 elimination samples); and
- about 26,450 of those 27,700 samples were being held by FSPs and about 1,250 'in force'.

[The position as at 31 August 2014 was that a total of about 19,200 DNA samples were being retained pursuant to the CPIA exception (some 1,260 being arrestee samples and some 17,940 elimination samples) and that of those retained samples some 18,780 were being held by FSPs and some 420 'in force'.]

ELIMINATION SAMPLES

186. As I indicated in my 2014 Report,[95] since August of 2013 and unless specifically instructed otherwise, FSPs have been retaining indefinitely all the elimination samples that have been submitted to them. This is, in my view, 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 have therefore pursued with the Home Office and others the possibility that a new retention policy should be adopted in relation to elimination samples and that revised guidance about them should be issued to forces.

187. It has recently been agreed that elimination samples should no longer be subject to a 'blanket' policy of indefinite retention and that they should only be retained beyond six months if the CPIA exception applies and the relevant force is satisfied that some genuine 'investigative purpose' will be served by their continued retention. It has further been agreed that, even in those circumstances, the continued retention of such samples should be reviewed on at least a quarterly basis and that steps should be taken to ensure that they are promptly destroyed if and when their retention ceases to be necessary.

188. A policy along these lines is to come into effect in January of 2016 with regard to 'new' elimination samples and it is anticipated that all 'legacy' elimination samples will have been reviewed – and that appropriate instructions will have been given in relation to them – by May of 2016 at the latest. Officials at the NDU and representatives of police forces and FSPs have clearly put a great deal of work into the design and implementation of this revised approach and I am hopeful that, as a result of their efforts, the unsatisfactory and anomalous treatment of elimination samples will soon become a thing of the past.

189. In my 2014 Report[96] I also expressed concerns about the wording of the pro-forma consent forms that are completed by the donors of elimination samples and I said that I understood that a new and more informative version of that form was soon to be introduced. Since then I have had extensive dealings with the NDU and others about how that form (and other forms which are completed by 'volunteer' donors of DNA samples) might usefully be amended, particularly so as to alert donors adequately to the true position as regards the retention of their samples.

190. A new and more suitable consent form has now been finalised in line with the new retention policy that is referred to above. I understand that that new form will be put into use early in 2016.

[95] (at paragraph 190)

[96] (at paragraph 191)

ARRESTEE SAMPLES

GENERALLY

191. The current Home Office guidance to forces in connection with the CPIA exception states:

> *"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."*

Given the relatively small number of arrestee samples that are apparently being retained pursuant to that exception, it seems that forces are attempting to act in accordance with that guidance and that they are giving careful thought to the retention of arrestee samples on that basis. It also seems clear, however, that forces have continued to take differing views of the true scope of that exception and that some forces continue to retain many more arrestee samples than other forces. Consequently – and as was the case last year – in the course of my visits to forces I have undertaken specific checks on their activities and policies as regards the retention of DNA samples in reliance on the CPIA exception.

DIP-SAMPLING AND DISCUSSIONS WITH FORCES

EAST MIDLANDS SPECIAL OPERATIONS UNIT

192. In April of 2015 I visited the East Midlands Special Operations Unit – Forensic Services (EMSOU-FS) in Nottingham. That unit provides and co-ordinates forensic services on behalf of five police forces i.e. Derbyshire, Leicestershire, Lincolnshire, Northamptonshire and Nottinghamshire. I met with the director and senior staff of EMSOU-FS and discussed with them, among other things, the (shared) policies of those forces as regards the retention of DNA samples pursuant to the CPIA exception.

193. On the date of my visit, 47 elimination samples were being held 'in house' by EMSOU on behalf of the five forces. Information was provided about those samples and I found no reason to suspect that they were being held otherwise than in accordance with PoFA.

194. Although no arrestee samples were at that time being held 'in house' by EMSOU pursuant to the CPIA exception, such samples were being held on behalf of the five forces by FSPs. Detailed information about those samples was unavailable at the time of my visit and I therefore arranged to carry out a dip sampling exercise at a later stage. In the course of that exercise I examined the position as regards 28 of the 550 arrestee samples that were being held by FSPs on behalf of those forces pursuant to the CPIA exception.

195. All of the arrestee samples selected proved to be less than 6 months old, the oldest having been taken just over 4 months previously. 5 had already been destroyed, 2 were already the subject of destruction requests, and 21 related to ongoing investigations where testing had already taken place or was considered to be a realistic possibility. It was clear that proper systems had recently been put in place to ensure that samples which were being

held pursuant to the CPIA exception were reviewed on a regular basis and I found nothing to suggest that those or other samples were being improperly retained by any of the 5 forces.

SUSSEX POLICE

196. In June of 2015 I visited the 'Forensic Investigations' unit which serves Sussex and Surrey Police. My visit focused primarily on Sussex Police but many of the matters which I discussed with the Head of Forensic Support Services and other key staff were also relevant to Surrey Police.

197. The great majority of the elimination samples which were being held in force by Sussex Police were under six months old and it was clear that effective recording and review mechanisms were in place in relation to them. The same was true as regards in-force holdings of arrestee samples, none of which was more than 3 months old.

198. At the time of my visit 132 arrestee samples were being held on behalf of Sussex Police by FSPs pursuant to the CPIA exception. I subsequently sought and obtained information about 15 of those samples. Although all of them had initially been required for forensic analysis and/or comparison, a review prompted by my visit had led Sussex police to the conclusion that 8 no longer needed to be retained. Monthly reviews of arrestee samples retained with FSPs have now been introduced.

MERSEYSIDE POLICE

199. In July of 2015 I visited Merseyside Police Headquarters and met with the Forensic Submissions Coordinator and other senior staff with responsibility for biometrics.

200. It was apparent from my visit that great care was being taken to ensure that arrestee samples are processed and quality-checked quickly and efficiently and none was being retained in-force at that time. It was also recognised, however, that more might usefully be done to ensure the proper recording and review of in-force holdings of elimination samples.

201. The force demonstrated robust processes for monitoring and reviewing arrestee samples retained with FSPs pursuant to the CPIA exemption and of the 20 cases examined I found no reason to suspect that the relevant samples were being held otherwise than in accordance with PoFA.

GWENT POLICE

202. During July of 2015 I also visited Gwent Police Headquarters. Gwent and South Wales Police work collaboratively in various areas and a Joint Scientific Investigation Unit (JSIU) has been in place since November of 2014. I met with the head of the JSIU and other key staff from the two forces.

203. It was apparent that, although real efforts had been made by Gwent Police to procure full compliance with PoFA, work remained to be done in terms of ensuring that 'legacy' material (including elimination samples) was not being improperly retained in-force.

204. As of 17 July 2015, 67 arrestee samples were being held at the JSIU for Gwent and 28 for South Wales: all were under 6 months old and none was being retained pursuant to the CPIA exception. As of 31 May 2015 only one arrestee sample was being held for Gwent Police by an FSP and that sample was being retained by Gwent on behalf of the British Transport Police.

205. I was satisfied that appropriate work was being undertaken by Gwent and South Wales Police to tackle compliance issues in general and issues relating to the CPIA exception in particular.

GREATER MANCHESTER POLICE

206. My final visit to a police force was to Greater Manchester Police (GMP), also in July of 2015. During it I met with the Head of Forensic Services for GMP and other senior staff with roles relevant to biometrics. It was clear that GMP had put in place a variety of policies and procedures to ensure that the force is PoFA compliant. It was in particular clear that there was a comprehensive system in place which covered the storage and review of elimination and arrestee samples held in-force pursuant to the CPIA exception.

207. At the date of my visit 2 arrestee samples were being held in-force pursuant to that exception. Those samples related to ongoing major crime investigations and I found no reason to suspect that they were being held otherwise than in accordance with PoFA.

208. On 21 July 2015 10 arrestee samples were being retained with an FSP. Data on those samples was not available at the date of my visit but was provided at a later date. Five of the 10 samples were at that time over 6 months old. My Office was subsequently informed that, following a force review of the relevant case details, all 10 of those samples had been destroyed.

CONCLUSION

209. In summary, then, save only that some 'legacy' samples stored in individual stations may have been overlooked and that the CPIA exception may sometimes be being misapplied, I have found no reason to suspect that there has been significant non-compliance with the sample destruction regime provided for by PoFA. I am satisfied, moreover, that in cases where deficiencies have been identified in the systems operated by the forces I have visited, those deficiencies have quickly been addressed.

210. 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 remains some uncertainty as to the circumstances in which it can properly be relied on;
- that forces differ substantially in their approaches to it; and
- that not all forces rigorously comply with their obligation to destroy both arrestee and elimination samples as soon as the CPIA exception ceases to apply.[97]

In those circumstances – and as I have mentioned above[98] – it remains my view that, as the Government appears to have recognised, clearer guidance should be issued as to the proper application of the CPIA exception.

4.2 DNA PROFILES AND FINGERPRINTS

BACKGROUND

211. 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.

212. 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.

213. 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.

[97] See section 63U of PACE (at subsection 5B) as amended by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014.

[98] See paragraphs 181-182 above.

HAVE DNA PROFILES AND FINGERPRINTS BEEN APPROPRIATELY DESTROYED/DELETED?

GENERALLY

214. As I reported in 2014 I have found no reason to doubt that, as was claimed by the Government, some 1,766,000 DNA profiles and some 1,672,000 fingerprints were deleted from the national databases in anticipation of the commencement of PoFA in October of 2013. As I also reported in 2014, however, the post-commencement position as regards the retention of such profiles and prints is significantly less satisfactory than that relating to the retention of DNA samples.[99]

215. It is clear that very considerable efforts were made prior to the commencement of PoFA 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, there are at least three reasons why that was always going to be an impossible task.

    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.[100]

    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,[101] 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 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.[102]

[99] See paragraphs 203-236 of my 2014 Report.

[100] I have continued to look into the issue of 'unlawful matches'. It is dealt with in more detail at paragraphs 263-267 below.

[101] See paragraph 25-28 above.

[102] See paragraph 56 above.

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 may well be retained on them and, just as important, profiles and prints that should have been retained on those databases may well be deleted from them.

216. In my 2014 Report I explained how problems had arisen in relation to each of those three matters. Regrettably, not all of those problems have yet been resolved and further such problems have become apparent in the course of this reporting year.

DELAYS IN UPDATING THE PNC

217. Significant delays in the updating of the PNC continue to be brought to my attention and it is my impression that they are still 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.

218. 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' (a 'UZ' marker) which will have the effect of precluding the automatic deletion of the relevant arrestee's biometric records. I am aware of more than one case in which a force has overlooked that deadline and, as a result, the arrestee's biometric records have been automatically deleted and the proposed application has had to be abandoned or withdrawn. I am also aware of one case in which biometric records were lost – and a section 63G application had to be withdrawn – because the force in question mistakenly applied a UZ marker to the PNC record of another individual with the same name as the subject of that application.

219. I have repeatedly raised my concerns about delays and/or errors in updating the PNC with officials at the Home Office, with the NDNAD Strategy Board and with others. Even so, it remains my perception that forces and/or individual officers are often unaware of the possible 'biometric' consequences of such delays and errors and that more could and should be done to draw them to their attention.

OTHER PNC PROBLEMS

220. In 2014 I referred to four matters relating to the programming and operation of the PNC which had proved to be problematic. Three related to matters which had 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 had 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. Two of these matters have now been resolved, two remain outstanding and five further PNC-related matters have now been brought to my attention. I deal first with the matters to which I referred in my 2014 Report.[103]

PROBLEMS IDENTIFIED IN MY 2014 REPORT

ERRONEOUS DELETIONS[104]

221. It came to my attention in early April of 2014 that the biometric material of around 30 individuals 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. I have been assured that this programming error has now been remedied. Regrettably, however, (and as is explained at paragraphs 229-239 below) it now appears that further PNC-related problems may well have led to the erroneous deletion of other (and more numerous) biometric records.

PROCEEDINGS STAYED[105]

222. A second problem associated with the programming of the 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 understand that all the necessary technical 'fixes' in relation to this problem are now fully in place.

'DISCONTINUED' ENTRIES[106]

223. A third problem associated with the programming of PNC became apparent in connection with 'Discontinued' 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). It was suggested that, on a 'worst case' estimate, this problem could have led to unlawful retention in about 140,000 cases but that the true figure was likely to be very much smaller.[107]

224. 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

[103] Further details about these problems can be found at paragraphs 212-222 of my 2014 Report.

[104] See paragraphs 213-214 of my 2014 Report.

[105] See paragraphs 215-217 of my 2014 Report.

[106] See paragraphs 218-220 of my 2014 Report.

[107] Even that 'worst case' estimate has now been reduced to 117,000 cases.

of such an entry but would thereafter be deleted unless they were subject to retention on some other grounds. Although it was originally anticipated that the necessary re-programming work would be completed by the end of 2014, it was later indicated that a 'prospective fix' would be introduced in August of 2015 and a 'retrospective fix' by the end of September 2015.

225. I have been informed that, whilst an intended prospective fix was indeed introduced in August of 2015, difficulties with the relevant software mean that this issue is in fact unlikely to be resolved – prospectively or retrospectively – before February of 2016. I have further been informed that, although it is likely that biometric records continue to be retained unlawfully as a result of this 'Discontinued' problem, it is possible that, as a result of those software difficulties, biometric records are also being lost from the national databases in circumstances where they should in fact be being retained.

226. I have asked to be kept abreast of developments in this connection and I shall, of course, continue to pursue the matter.

WANTED/MISSING MARKERS

227. A further PNC-related problem to which I referred in my 2014 Report 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. In my 2014 Report I observed that it seemed likely that in April of 2014 the biometric records of approximately 4300 individuals were being wrongly retained as a result of this problem; in October of 2015 the relevant figure seems likely to have been approximately 4,650.[108]

228. Although I understood at the time of my 2014 Report that it was unlikely that this 'Wanted/Missing' problem could wholly be resolved – and thus that it was probable that it would continue to prevent the automatic deletion of at least some biometric records that could not lawfully be retained – I also understood that work which was due to be carried out during 2015 was likely to reduce by over 95% the number of records that were affected by the problem. In the event, however, it seems that this work will not now be done before April of 2016 at the earliest. In the meantime further examples of erroneous retention as a result of Wanted/Missing markers will no doubt come to light: one which has done so relatively recently is described in detail at paragraphs 63 and 64 above.

PROBLEMS IDENTIFIED SINCE MY 2014 REPORT

229. Since preparing my 2014 Report I have become aware of a number of further problems affecting the retention of biometric records which have arisen out of difficulties relating to

[108] I am again very grateful to David Low, Specialist PNC Policy Advisor for the Metropolitan Police, for the assistance he has given me in relation to this matter.

the programming and/or operation of the PNC. Only the first two of those problems have as yet been resolved.

PROBLEMS ASSOCIATED WITH HISTORIC 'WORKAROUNDS' AND MULTIPLE ARRESTS

230. Even before PoFA came into effect it was recognised:

- that the software that had been developed to drive the retention and deletion of biometric records would not always generate the correct result in cases where so-called 'workarounds' had been applied to the PNC or where an individual had been arrested on more than one occasion; and
- that in such cases biometric records might be inappropriately retained or deleted.

Work was undertaken to address that deficiency and by the time PoFA commenced some 7,300 affected cases had been identified and 'fixed'.

231. It later became apparent that, on a 'worst case scenario', up to 75,000 other cases might have been affected by this problem and that more extensive re-programming work would therefore be required. I understand that that work, which provided both a retrospective and a prospective solution to the difficulties which had arisen, was completed on 12 August 2015. I further understand that it now seems clear that no more than about 5,900 other cases had in fact been affected by that problem.

'WITHDRAWN – OTHER' AND 'DISCHARGED – OTHER' ENTRIES

232. When I learnt in 2014 of the problems associated with 'Discontinued' entries which are referred to at paragraphs 223-226 above, I was not aware that, even before PoFA came into effect, broadly similar problems had been identified in connection with 'Withdrawn – Other' and 'Discharged – Other' entries on the PNC. Nor was I aware that it had at that time been decided that those problems would be addressed by introducing a programme whereby biometric records are retained for a minimum of twelve (rather than six) months after the making of such entries. Whilst it is perhaps surprising that no mention was made of those matters to me – and that different minimum retention periods are to apply in what appear to be very similar circumstances – I am satisfied that nothing of substance turns on those points.

233. An additional problem later became apparent as regards the retention of biometric records in circumstances where a 'Withdrawn – Other' or 'Discharged – Other' entry had been made on PNC. Put shortly, that problem was that, contrary to what had been intended, DNA profiles which were affected by those entries became unsearchable on the national database shortly after they were loaded to it (i.e. immediately after they had been speculatively searched against other profiles on that database). There is, of course, little point in retaining profiles on the national database if they are not searched against when later crime scene profiles are added to it.

234. I understand that that additional problem has now been fixed and that all such DNA profiles have been fully searchable since late September of 2015. I further understand that, although about 200 cases a month may have been affected by this issue, only about 40 relevant cases were in fact identified and that no relevant 'hits' have come to light.

COUNTS LEFT TO 'LIE ON THE FILE'

235. In cases where an indictment contains a number of counts, it is not unusual for a defendant to be convicted of some of those counts and for others which have not been dealt with to be left to 'lie on the file' (i.e. for an order to be made whereby the prosecution may in certain circumstances be able to pursue those counts at a later stage). However, in some cases – one of which was brought to my attention in March of 2015 – counts may be ordered to 'lie on the file' even in circumstances where the defendant has not been convicted of an offence. As things currently stand, a 'lie on the file' entry on the PNC will cause biometric records to be retained indefinitely even if – as in the case which was brought to my attention – they should in fact have been deleted.

236. It seems extremely unlikely that there are or will be many cases in which biometric records are wrongly retained as a result of this programming rule.

MINORS WHO HAVE MULTIPLE CONVICTIONS

237. As is indicated at paragraph 13 above, special retention rules apply as regards the biometric material of those who have been convicted of offences while under the age of 18. In some of those cases a five year retention period will apply whereas in others – and particularly where the minor has been convicted on more than one occasion – the material may be retained indefinitely.[109]

238. It was brought to my attention in October of 2015 that the relevant software calculates incorrect retention periods for offenders under the age of 18 who have multiple convictions and that, as a result, a second or later conviction of such an offender will only attract a 5-year retention period rather than indefinite retention. I understand that, although the precise cause and scale of this problem have yet to be established, it may affect up to 50,000 records which are currently shown on PNC as attracting a 5 year retention period and that it has almost certainly led – and will almost certainly lead – to the erroneous deletion of large numbers of DNA profiles and fingerprints from the national databases.

239. I have recently been informed that a suitable fix to this problem should be delivered in February 2016. I will again keep it under review.

[109] Moreover, if a custodial sentence has been imposed, the material may be retained until 5 years after the end of that sentence.

ONGOING INVESTIGATIONS AND THE RELEASE OF ARRESTEES OTHERWISE THAN ON BAIL

240. At paragraph 56 above I referred to problems which have come to light in connection with protracted investigations.[110] Put shortly, those problems have arisen as a result of the following.

i. Although police forces clearly feel under pressure to minimise the periods for which arrestees are kept on police bail, there appears to be widespread uncertainty as to whether or not an arrestee can properly be released from bail in circumstances where the relevant investigation is still ongoing and the arrestee remains a suspect for the offence at issue. In the absence of clarity in that regard – and although some consider it unacceptable to do so – it is not uncommon for forces to adopt that course (i.e. to release arrestees who are still under investigation otherwise than on police bail).

ii. Many forces have custody IT systems which are linked to the PNC in such a way that the closure or cancellation of an arrestee's bail record will automatically generate an NFA entry on the PNC. This will happen even in circumstances where no decision has actually been made about the case and the arrestee has specifically been told that he or she remains under investigation.

iii. When an NFA entry is generated on the PNC – and unless some other step is taken – the arrestee's biometric records will quickly be deleted from the national databases save only if they are subject to retention for some other reason (e.g. because the arrestee has previously been convicted of a recordable offence).

iv. By section 63E of PACE (as amended by 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. Whilst the making of an NFA entry on the PNC will usually indicate that an investigation has indeed reached a conclusion, it will not do so in circumstances such as those at issue. It therefore follows that the 'automatic' deletion of an arrestee's biometric records in those circumstances will be inappropriate and premature.

v. As is pointed out at paragraphs 92-93 above, on the face of things the police have no power to require an individual who they have arrested to provide a second DNA sample (or indeed a second set of fingerprints) simply because the profile derived from the sample which was taken from that individual when they were first arrested (or the set of fingerprints which was taken from him or her on that occasion) has been deleted from the relevant database in circumstances where it could in fact have been retained.

vi. It follows that in cases of this type the biometric records of an arrestee may well be deleted – and 'replacement' biometrics may well be unobtainable from that arrestee

[110] See also in this regard paragraphs 25-28 above.

– even though he or she has at all times remained under investigation and even though it is clear from the relevant legislation that those biometric records could lawfully have been retained by the police.

241. Over the past few months I have become aware of a number of cases where biometric material has been lost – or at risk of loss – as result of this problem and I have little doubt but that there have been numerous other cases in which, by this route, unnecessary (and probably unnoticed) deletions have been triggered unwittingly by forces.

242. It has also become apparent to me that, whilst some forces are almost certainly unaware of the 'biometrics' consequences that may flow from the releasing of arrestees otherwise than on police bail, other forces have taken active steps to avoid them. Thus, of the forces which I know to release arrestees otherwise than on bail in circumstances where investigations are ongoing:

    i. some manipulate the interface between the force custody system and the PNC so as to ensure that the closure of the custody record does not automatically update the relevant PNC record as 'NFA';

    ii. some allow the custody record automatically to update the PNC with an NFA disposal but then immediately manually amend that PNC disposal so as to remove the NFA disposal and to show the case as still pending; and

    iii. some allow the custody record automatically to update the PNC with an NFA disposal but then immediately add a 'Biometrics Commissioner' or other 'marker' to the PNC record to ensure that the biometrics are retained.

    There are arguments for and against each of those approaches but in my view it is clearly desirable that, whichever of them is adopted, forces ensure that every case in which an arrestee is released otherwise than on bail is subjected to a process whereby the progress of the case and the PNC entries in respect of it are reviewed on a regular basis.

243. I have repeatedly raised this 'no bail' problem with Home Office officials and others and I have repeatedly pressed for appropriate guidance to be issued as regards:

    - the propriety/acceptability of releasing arrestees otherwise than on bail in circumstances where they are still under investigation; and
    - the practical steps that should be taken by forces to avoid any unwelcome 'biometric' consequences of doing so.

    I have also repeatedly emphasised that consideration should be given to this problem – and to the revision of any such guidance – if and when (and as is apparently intended) changes are made to the law relating to police bail.[111] I shall continue to keep this problem – and any steps which are taken by the Home Office in relation to it – under careful review.

[111] See e.g. https://www.gov.uk/government/publications/queens-speech-2015-what-it-means-for-you/queens-speech-2015-what-it-means-for-you#policing-and-criminal-justice-bill at paragraph 18.1 and

BIOMETRICS COMMISSIONER (UZ) MARKERS

244. As is mentioned at paragraph 28 above, 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' (a 'UZ' marker) which will have the effect of precluding the automatic deletion of the relevant arrestee's biometric records. I am provided by ACRO with a monthly report which gives brief details of every UZ marker that appears on the PNC. This report enables me to monitor the number of UZ markers in use and to check the data provided against my own records.

245. Among the points which have emerged from my analysis of these monthly reports are the following.

i. There have been numerous instances of the inappropriate use of a UZ marker, for example where a police officer has misunderstood the purpose of such a marker or, more commonly, where a UZ marker has simply been erroneously applied. Where this has come to my attention I have informed the relevant police force of the mistake and the marker has usually been removed immediately. There was, however, a recent instance in relation to a police force which had for some months had three UZ markers present on the PNC in circumstances where no application had been made or notified to me. Although these markers have now been removed after numerous prompts to the force concerned, it seems almost certain that the relevant biometrics were being held unlawfully through much of that period;

ii. A common problem is that the retention date associated with a UZ marker on the PNC is incorrect. The cause of this problem seems to be that when a UZ marker is applied to the PNC the 'end date' for retention is automatically set at three years from the date the marker was applied to the record. That end date then needs to be changed manually to reflect the fact that, if a section 63G application is successful, PoFA allows for the biometrics to be retained only for three years from the date they were taken.[112] It seems that this small but important point is often overlooked and, although appropriate changes have usually been made soon after I have alerted forces to these incorrect dates, there have been instances where several months have passed before this has been done.

iii. On a number of occasions UZ markers have been placed on the PNC in order to avoid the inappropriate deletion of biometrics in cases where, notwithstanding the fact that an NFA entry has been made on the PNC, the relevant investigation in reality remains ongoing. Cases of that sort are referred to at paragraphs 56 and 242(iii) above and I keep such cases under careful review. Although I remain content for UZ

---

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/418226/150323_Pre-Charge_Bail_-_Responses___Proposals.pdf at page 7.

[112] (though note in this connection footnote 16 above)

markers to be used in such circumstances with my specific permission, my hope is that guidance will soon be given as to better ways of avoiding inappropriate deletions of that sort.[113]

COPIES

246. Section 63Q of PACE (as amended by PoFA) 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."*

247. As regards copies of DNA profiles and fingerprints, I have little of substance to add to the observations I made at paragraphs 224-231 of my 2014 Report. Put shortly, it remains the case that, save only for copy fingerprints that are being retained on national fingerprint training databases, in the National Fingerprint Archive or in case files, I have no reason to suspect significant non-compliance with section 63Q of PACE. It is also the case:

- that I have seen nothing to suggest that any copy fingerprints that are being unlawfully retained are being used improperly;
- that the cost and effort that would be required to 'cleanse' those training databases, that Archive and/or case files of any unlawfully retained copy fingerprints would be very considerable indeed; and
- that work on the replacement of the training databases is already underway and that efficient and effective safeguards have already been established as regards the National Fingerprint Archive.

248. None of the police forces which I have visited during this reporting year maintains its own searchable database of fingerprints and each of them appears to have in place proper processes to ensure the identification and destruction of hard copy fingerprints which should no longer be being retained. The processes in place at the National Fingerprint Archive – which I also visited – are rather less straightforward.

249. At paragraphs 227-229 of my 2014 Report I explained that it was likely that up to around 154,000 'unreconciled' fingerprint records which were being stored in the National Fingerprint Archive were records which could not lawfully be retained under the PoFA regime. I also explained that it would apparently 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. With the endorsement of the Information Commissioner's Office it was agreed that, rather than embarking on such an

[113] See e.g. paragraph 243 above.

exercise, safeguards would be introduced whereby, when forces sought access to records in that collection:

- checks would be made as to whether or not the copy fingerprints at issue were in fact copies which fell for destruction under (new) section 63Q(1) of PACE;

and, if that proved to be case,

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

I understand that, in the event, not a single request for 'unreconciled' fingerprints has yet been made.

250. I visited the Archive in May of 2015 and I was impressed by the care which is taken by its staff to ensure that hard copy fingerprints which should have been destroyed are not released to requesting forces. Even so, however, I have made various recommendations to them as to how their processes and procedures might usefully be clarified and/or improved.

CONCLUSION

251. 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.

252. Given the complexities of the retention regime and 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. In the event – and despite the considerable efforts that have been made to minimise those wrongful retentions and deletions and to address their causes – it seems likely:

- that a significant number of DNA profiles and fingerprints which should have been retained on the national databases have in fact been deleted;
- that thousands of profiles and prints which should have been deleted have in fact been retained; and
- that errors of this sort are continuing to occur and that some of the problems which have given rise to them have yet to be resolved.

I shall of course continue to monitor these PNC-related issues and to press for them to be resolved as quickly as possible. I am particularly concerned about the continuing and unresolved problems which are referred to at paragraphs 223-226, 227-228, 237-239 and 240-243 above.

253. Although it would be unrealistic to imagine that retention errors can be avoided completely, it seems clear that more could be done to minimise them, particularly by way of re-

programming work to the PNC. Whilst I recognise that differing views could sensibly be taken as to the extent to which limited resources should be devoted to such work, one useful step which could and should be taken – and which would involve minimal expenditure – would be for the Home Office to do more to alert forces to the problems and risks that have been identified as regards biometric retention and to ensure that more and clearer guidance is issued as to the steps that forces can and should take to avoid them.

254. It also seems likely that substantial numbers of hard copies of fingerprints are being retained otherwise than in compliance with the PoFA regime. I have, however, no reason to suspect that improper use is being made of those hard copies and am satisfied that reasonable steps have been taken to avoid such a situation arising. I shall also continue to keep this matter under careful review.

4.3 EARLY DELETION OF BIOMETRIC RECORDS BY ORDER OF A CHIEF OFFICER

GENERALLY

255. Although it is open to an individual to apply to the police for the 'early' deletion of their biometric records from the national databases – i.e. for their deletion even though continued retention would be lawful under the regime established by PoFA – the circumstances in which requests of that sort can be granted are very limited indeed. I addressed that issue at paragraphs 237-244 of my 2014 Report and observed, among other things:

- that it is not difficult to conceive of circumstances in which the continued retention of an individual's biometric records might reasonably be considered unnecessary and disproportionate even though those records are being lawfully retained;
- that such circumstances might well arise, for example, where the continued retention of the material 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;
- that the guidance which was at that time in place – and which Chief Officers were legally obliged to follow – precluded the possibility of early deletion in those and other circumstances where such deletion might well be thought appropriate; and
- that in my view a significantly less restrictive approach should be taken to requests for early deletion.

In the Government's response to my Report Lord Bates noted my observations in this connection and indicated that he had *"asked ... officials to give this matter further consideration and discuss the issue with police and other relevant stakeholders to consider a way forward."*

256. Since that time – and as was anticipated in my Report[114] – replacement guidance has been issued in respect of applications for the early deletion of biometric records and that revised guidance now also covers applications for the early deletion of PNC records. As was also anticipated in my Report, however, the substance of that guidance remains unchanged.[115] Although I am unaware of any discussions having taken place with police or other stakeholders about the possible adoption of a less restrictive approach to requests for early deletion, I understand that the existing policy is currently subject to challenge in the context of Judicial Review proceedings.

WRONGFUL ARRESTS AND MISTAKEN IDENTITY

257. At Section 63D(2) of the Police and Criminal Evidence Act 1984 (as introduced by section 1 of PoFA) it is provided that:

> "*Fingerprints and DNA profiles ... must be destroyed if it appears to the responsible chief officer of police that –*
>
> *(a) the taking of the fingerprint or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful, or*
>
> *(b) the fingerprint was taken, or, in the case of a DNA profile, was derived from a sample taken, from a person in connection with that person's arrest and the arrest was unlawful ... ."*

In that connection the current guidance as regards 'early/exceptional deletion' further states that:

> *"The deletion must occur as soon as the information comes to the Chief Officers' attention. An application for record deletion is not necessary in these circumstances."*

258. ACRO has asked for guidance from the Home Office as to whether or not there is an obligation on forces to delete such biometrics otherwise than in cases where an allegation of unlawful taking, wrongful arrest or mistaken identity has been specifically raised with the responsible Chief Officer (i.e. whether forces are required to search proactively for such cases). It has been suggested that, if that were to be the case, it might well be appropriate to alert forces (and Chief Officers) to such cases by way of an appropriate disposal option on the PNC.

259. I understand that ACRO has yet to receive a substantive response to its enquiry.

[114] See footnote 92 of my 2014 Report.

[115] See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430095/Record_Deletion_Process.pdf.

5. THE USE TO WHICH BIOMETRIC MATERIAL IS BEING PUT

5.1 GENERALLY

260. 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]"*.

261. 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."*

262. 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 section 63T(1). As regards section 63T(2), however, three matters relating to the use to which biometric material is put appear to me to merit particular mention. They are:

- unlawful matches;

- 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 UNLAWFUL MATCHES

263. As I have explained at Section 4 of this Report, it seems likely that, mainly as a result of PNC-related problems, large numbers of DNA profiles and fingerprints which should have been deleted from the national databases have in fact been retained on them. All or most of those wrongfully-retained biometric records are searched against automatically when new (crime scene or other) profiles and prints are loaded to those databases and from time to time 'matches' are found. Those matches (i.e. matches with unlawfully held material) are known as 'unlawful matches'.

264. Even before PoFA came into effect it was recognised that at least some unlawful matches were likely to occur and, shortly after 31 October 2013, guidance about such matches was issued by the Home Office. That guidance[116] (which remains in effect):

- referred forces to section 63T(2) of PACE (which provides that "*Material which is required to be destroyed ... must not at any time after it is required to be destroyed be used ... for the purpose of the investigation of any offence"*; and
- made specific recommendations as to the checks which a force should undertake when a match is found so as to satisfy itself that the relevant biometric material was being lawfully held when the search which led to that match was carried out.

In the penultimate paragraph of that document it was noted that the guidance had *"been created to assist forces to process forensic matches safely and to ensure that any identifications reported to investigating officers comply with the provisions of PoFA (as much as possible)."*

265. A number of unlawful matches have come to my attention since October of 2013 and it must be possible that others have occurred which have gone unnoticed by the forces concerned. More importantly, however, it has become apparent to me that when unlawful matches are discovered – and notwithstanding section 63T(2)(b) – at least some forces are communicating those matches to the relevant investigating officers, albeit subject to caveats such as:

> "*This match is communicated for intelligence purposes only to generate further investigative lines of enquiry. It cannot be acted on in isolation and further enquiries will be required*."

Since it appears that the only possible reason for communicating such a match to an investigating officer – even 'for intelligence purposes only' – will be to assist his or her

[116] *'Protection of Freedoms Act: Regulation of Biometric Data – destruction, retention and use of fingerprints etc. Guidance to ensure forensic matches are lawful post commencement.'*

investigation of the relevant offence, it seems strongly arguable that forces which adopt this course are using unlawfully held biometric material in a manner which is contrary to s.63T(2)(b).

266. Whilst it might reasonably be inferred from the guidance referred to above that unlawful matches should not be reported to investigating officers, there is no express provision to that effect and no clear indication or explanation of the practical steps and actions that forces should take – or not take – in the event that unlawful matches are discovered. I am concerned that that lack of clarity, particularly as regards the communication of such matches to investigating officers, may be leading forces to adopt differing (and possibly unlawful) policies.

267. Although I have raised these concerns with Home Office officials on a number of occasions since August of 2015, I have yet to receive a substantive response to my enquiries and the relevant guidance remains unchanged. In my view that guidance should be revised – and clearer and more precise guidance on this point should be issued – as a matter of some urgency.

5.3 SPECULATIVE SEARCHES

BACKGROUND

268. 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 speculative 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.

269. At paragraphs 248-272 of my 2014 Report I described in some detail the processes by which speculative searches are carried out and I addressed a number of issues which had arisen in relation to them. Among other things I reported in particular:

- that discussions were ongoing between the MPS and the Home Office as to whether or not more time should be allowed for the carrying out of speculative searches following arrests for non-qualifying offences;[117] and

[117] See paragraphs 267-270 of my 2014 Report.

- that the guidance issued by the Home Office about the process which should be followed when a speculative search results in a confirmed (lawful) match appeared to me to be at odds with the relevant provisions of PACE.[118]

I also observed that it seemed to me surprising – and on the face of things undesirable – that 'ten-print to crime scene mark' searches were not always launched immediately when an arrestee's fingerprints were taken.[119]

DEVELOPMENTS

EXTENDING THE TIME FOR SPECULATIVE SEARCHES

270. Although in the Government's response to my Report in March of 2015 Lord Bates indicated that the Government would *"consult with stakeholders and consider carefully the arguments for and against extending the 14-day retention period for qualifying offences to non-qualifying offences"*, I am unaware of any such consultation having taken place. I understand, moreover, that although the MPS wrote to the Home Office about this matter in March of 2014 and again in October of that year, it has yet to receive a substantive reply to those letters. [Equally, however, it remains the case that no other force has raised the matter with me and that none of those I have visited has, when questioned about it, suggested that the existing time limit has caused it significant difficulty or concern.]

THE NEED FOR AN ARREST

271. At paragraph 272 of my 2014 Report I observed as follows.

> "*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[ly] 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*[120] *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*."

In the Government's response to my Report in March of 2015, Lord Bates indicated that he had asked his officials "*to look into this matter further*".

---

[118] See paragraph 272 of my 2014 Report. That guidance is entitled: *"Protection of Freedoms Act: Regulation of Biometric Data – destruction, retention and use of fingerprints. Single Search - Guidance to forces*."

[119] See paragraphs 253 and 271 of my 2014 Report and paragraphs 273-275 below.

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

272. Although it is now more than 15 months since my Office first raised this matter with the Home Office – and although we have raised it again on numerous later occasions – I have yet to receive a substantive response to my enquiries and the guidance in question remains in force in unamended form. In this regard too, then, it seems strongly arguable that forces are using biometric material in a manner which is contrary to section 63T(2)(b).

SPEED OF SEARCHING

273. In my 2014 Report I observed as follows.

> "*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*.
>
> ...
>
> *270. 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.*"

274. I have raised this issue with each of the police forces which I have visited this year and I have been told that, with only one exception, it is the practice of each of them to launch a 'ten-print to crime scene mark' search automatically from Livescan. Those forces all indicated that they considered such an approach to be obviously desirable whereas the other force expressed the view that it was inappropriate to launch such a search unless – and as was not for it the position at weekends – relevant experts were in a position to review the results immediately.

275. Whilst these issues clearly fall outwith the ambit of my responsibilities, it may be that the Home Office and/or the College of Policing will wish to consider whether any – and, if so, what guidance should be issued to forces in relation to them.

5.4 INTERNATIONAL DATA SHARING

GENERALLY

276. One aspect of my oversight role as regards the use to which biometric material is being put is that of overseeing the sharing of such material internationally. The Home Office's *International DNA Exchange Policy for the United Kingdom*[121] states that:

> *"The Biometric[s] Commissioner ... will dip sample cases in which DNA material has been exported from the UK to make sure that this has been done appropriately."*

Although there is 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.

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

POLICY REVIEW

278. Last year representatives of the NCA and others raised with me various issues relating to the operation of the then relevant policy (i.e. the '*Home Office DNA Searching Policy for the United Kingdom*'). In particular, it was apparent that there was uncertainty as to when and how, under that policy, information that would identify an individual ('demographic information') could properly be released to foreign law enforcement agencies following a biometric match against the UK National DNA Database. Among other things, that uncertainty had led to a significant delay in the sharing of potentially valuable information about a serious crime with a foreign police force.

279. I was of course concerned that the policy governing the international exchange of DNA profiles and associated demographic information should not – whether in reality or perception – unnecessarily impede the progress of investigations. I raised that concern with officials from the NDU[122] in December 2014 and I recommended that they re-visit that policy, particularly with a view to clarifying the position as regards the disclosure of demographic information after an actual or possible biometric match. In consultation with the NCA and other interested parties the NDU then set about the drafting of a comprehensively revised policy, the '*International DNA Exchange Policy for the United Kingdom'*, and that new (and, in my view, much improved) policy was issued in October 2015.

[121] https://www.gov.uk/government/publications/international-dna-exchange-policy-for-the-united-kingdom

[122] i.e. National DNA Database Delivery Unit.

THE ROLES OF THE UKICB AND ACRO

280. The UK International Crime Bureau (the UKICB) 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, most requests for the international exchange of DNA profiles are channelled through the UKICB. The UKICB also deals with the international exchange of fingerprints for intelligence purposes.

281. 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.[123]

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

282. 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

283. 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 410 sets of fingerprints relating to (non-UK) EU nationals are currently sent each month to EU member states in connection with Requests Out.[124]

[123] Problems which have arisen as regards those matters are addressed at paragraphs 68-83 above.

[124] (i) Although this 'average' figure is accurate, it should be noted that – as with other 'average' figures in this section – there are substantial fluctuations in the actual figures from month to month.

(ii) 4469 fingerprint sets were exported between January and November of 2015. Comparable figures for the period January 2014 to December 2014 were 1,360 sets or approximately 110 sets per month. It seems likely that this substantial rise is at least in part due to the increase in criminal records checks being performed by police in England and Wales following arrests of foreign nationals. (See further at paragraph 83 and footnote 45 above.)

284. 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 subject's convictions (if any) in the UK and will sometimes be accompanied by the subject's fingerprints. These fingerprints are used to carry out a 'hit/no hit' search on IDENT1. On average, approximately 4 sets of fingerprints are currently received each month from other EU member states in connection with Requests In.[125]

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

NOTIFICATIONS

286. 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 630 sets of fingerprints relating to convicted (non-UK) EU nationals are sent each month to EU member states and Interpol in connection with Notifications.[126]

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

288. 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: on average only around twice per month.[127] The relevant conviction information is loaded to the PNC and, when fingerprints are received, they are loaded to IDENT1.

EXCHANGES WITH NON-EU COUNTRIES

289. 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 1,345 sets of fingerprints relating to foreign nationals are currently sent each month to non-EU countries in connection with Requests Out;[128]
- approximately 95 sets of fingerprints are currently received each month from non-EU countries in connection with Requests In;[129]

[125] 48 fingerprint sets were received between January and November of 2015. Between January and December of 2014 the comparable figure was 237.

[126] 6,954 fingerprint sets were exported between January and November of 2015. Comparable figures for the period January 2014 to December 2014 were 13,306 sets or approximately 1,100 sets per month.

[127] 24 fingerprint sets were received between January and November of 2015. Between January and December of 2014 the comparable figure was 25.

[128] 14,774 fingerprint sets were exported between January and November of 2015. Comparable figures for the period January 2014 to December 2014 were 12,060 sets or approximately 1,005 sets per month.

- approximately 265 sets of fingerprints relating to non-UK nationals are currently sent each month to non-EU countries and Interpol in connection with Notifications;[130] and
- it is rare for fingerprints to be received from non-EU countries in connection with Notifications.[131]

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

EXCHANGE OF DNA AND FINGERPRINTS FOR INTELLIGENCE PURPOSES

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

DNA SAMPLES

291. DNA samples are very rarely exchanged. The UKICB 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.

292. No DNA samples were exported between 1 September 2014 and 31 August 2015.

DNA PROFILES

293. 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 Exchange Policy for the United Kingdom* imposes strict limitations on the circumstances in which profiles may be exchanged.

294. There are 4 types of DNA profile enquiry that are dealt with by the UKICB.[132]

OUTBOUND SUBJECT PROFILES

295. The DNA profile of a known individual is sent abroad only with the express approval of the data owner for the DNA profile[133] and the NDNAD Strategy Board. A risk assessment must

[129] 1,044 fingerprint sets were received between January and November of 2015. The comparable figure for the period January to December 2014 was 682 or approximately 60 sets per month. ACRO provides the 'Requests In' Service to the NCA and therefore receives these requests directly from the NCA.

[130] 2,923 fingerprint sets were exported between January and November of 2015. Comparable figures for the period January 2014 to December 2014 were 6,638 sets or approximately 555 sets per month.

[131] The total figure for January to November of 2015 was 8. The comparable figure for January to December of 2014 was 33. I 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.

[132] 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.

be conducted and the force must explain why it believes that sending the profile to the specified country (or countries) is appropriate.

296. The Home Office's Policy for the United Kingdom states that:

> *"A named person's DNA profile should only be exported when such a course is necessary, reasonable and proportionate ... and meets one or more of the following criteria:*
>
> *1 It is for purposes related to the prevention or detection of crime;*
>
> *2 It is for purposes related to the identification of a dead person;*
>
> *3 It is in the interests of National Security; or*
>
> *4 It is for the purposes of a Counter-Terrorism investigation."*

Cases where subject profiles have been sent abroad are relatively rare: between 1 September 2014 and 31 August 2015 only 13 DNA subject profiles were sent abroad.

INBOUND SUBJECT PROFILES

297. 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 normally only comply with a request for the searching of an inbound person, crime stain or unidentified body DNA profile, where:*
>
> *1 the offence allegedly committed would be a qualifying offence ... if it were committed in the UK,*
>
> *2 the profile is derived from a missing person or unidentified body;*
>
> *3 the request and any subsequent search is necessary, reasonable and proportionate; and*
>
> *4 the DNA profiles meet the UK minimum quality criteria for searching.*
>
> *Any requests that do not meet these criteria will be considered on a case by case basis and may be referred for specific authorisation to the NDNAD Strategy Board."*

DNA person profiles from other countries are currently received at an average rate of approximately 9 per month.[134]

OUTBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

298. 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 normally satisfy itself that:*
>
> - *the crime under investigation is a UK Qualifying Offence ...;*
> - *the DNA profile is lawfully retained on the UK NDNAD;*

[133] The Chief Officer of the law enforcement agency that collects a DNA sample is the data owner for the DNA profile that is derived from it.

[134] 108 subject profiles were received between 1 September 2014 and 31 August 2015.

- *there is good reason to believe that the material from which the DNA profile was generated was directly associated with the perpetrator of the crime ; and*
- *there is good reason to believe that the proposed international search may assist in the investigation of that crime."*

DNA crime scene profiles, including those from unidentified bodies, are sent to other countries at an average rate of around 7 per month.[135]

INBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

299. DNA crime scene profiles or unidentified body profiles may be received from abroad. The Home Office Policy states that, absent specific authorisation by the NDNAD Strategy Board, the UK will normally only comply with a request for the searching of an inbound crime scene profile if the relevant crime meets the definition of a 'UK Qualifying Offence'.[136] In every case consideration will be given to the question of whether or not "*the request and any subsequent search is necessary, reasonable and proportionate*".

300. DNA crime scene profiles from other countries, including those from unidentified bodies, are currently received at an average rate of around 46 per month.[137]

FINGERPRINTS AND FINGERMARKS

301. There are 4 types of fingerprint enquiry dealt with by the UKICB:

OUTBOUND FINGERPRINTS

302. 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.

303. 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

[135] 81 crime scene/unidentified body profiles were exported between 1 September 2014 and 31 August 2015. 1 of those profiles related to an unidentified body.

[136] It seems that, as a general rule, the UKICB will also agree to the searching of an inbound crime scene profile if the relevant offence falls within the ambit of a list of serious offences which has been approved by the Home Secretary. I have referred to that list at paragraph 76 above and my enquiries into this issue are ongoing. I have little doubt but that, even if this practice is not in strict compliance with the new Home Office Policy, such searching would be specifically authorised by the NDNAD Strategy Board.

[137] 556 crime scene profiles/unidentified body profiles were received between 1 September 2014 and 31 August 2015. 45 of those profiles related to unidentified bodies or human remains.

Superintendent for non-EU countries) which addresses relevant Human Rights issues in the country or countries to which the fingerprints are to be sent.

304. Outbound fingerprint requests are currently processed at an average rate of around 130 per month.[138]

INBOUND FINGERPRINTS

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

306. Inbound fingerprint requests are currently received at an average rate of around 50 per month.[139]

OUTBOUND CRIME SCENE FINGERMARKS

307. Requests to send crime scene fingermarks to other countries are rarely made: certainly less often than once a month.[140]

INBOUND CRIME SCENE FINGERMARKS

308. Inbound requests to search crime scene fingermarks against IDENT1 are currently received at an average rate of around 7 per month. I understand that, as with crime scene DNA profiles, foreign crime scene fingermarks will normally 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.[141]

DIP SAMPLING

309. During a visit to the offices of the UKICB in November of 2015 my Head of Office dip-sampled – and then reported to me on – 15 cases in which DNA profiles and/or fingerprints had been exchanged internationally. In 8 of those cases DNA profiles or fingerprints had been transferred out of the UK.

310. Although no cause for concern was found in 14 of the 15 cases sampled, concerns did arise in relation to one case where an individual's DNA profile was exported from the UK (for searching abroad) with associated demographic information. Further work is ongoing in respect of that case and in respect of other matters which arose out of that visit.[142]

---

[138] 1,048 ten-print records were exported between 1 January to 31 August 2015.

[139] 404 ten-print records were received between 1 January and 31 August 2015.

[140] Latent marks were exported on 43 occasions between 1 January and 31 August 2015. 36 of those exports were in relation to the same case reference.

[141] However, as with inbound crime scene profiles, it seems that the UKICB will also agree to the searching of an inbound crime scene fingermark if the relevant offence falls within the ambit of a list of serious offences which has been approved by the Home Secretary. See in this regard footnote 136 above.

[142] I am grateful to the officials at the NCA for their assistance during that visit and more generally.

EUROPEAN ARREST WARRANTS

311. The UKICB 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 individuals. 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).

312. The UK joined the law enforcement element of the Schengen Information System (SIS II) on 13 April 2015. This is a Europe-wide means of sharing information about EAWs to assist law enforcement and border control. The NCA operates the UK's Sirene Bureau[143] and is responsible for recording all requests received through the SIS II. All EAW requests, whether or not they have a UK connection, are now recorded and this has resulted in a higher number of recorded requests in 2014/15 than in previous years.[144]

313. For outgoing EAW requests, fingerprints relating to the subject are sent to the country in question using SIS II. Those fingerprints must likewise be deleted from the receiving country's database at the end of the process.

314. It appears that in the calendar years 2010 to 2014 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. In the fiscal year 2014-15, EAW requests received increased from 7881 in 2013/14 to 12,134.[145]

PRÜM

315. The Prüm Council Decisions of 2008[146] allow for the reciprocal searching of DNA and fingerprint databases within the EU on an anonymised 'hit/no hit' basis. As I explained in my 2014 Report[147], those Decisions were subject to the UK's opt-out under Protocol 36 of the Lisbon Treaty and on 10 July 2014 the Home Secretary stated:

> *"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*

[143] 'Sirene' stands for 'Supplementary Information Request at the National Entries'. Each member state which operates the SIS II has set up a national Sirene Bureau that is responsible for any supplementary information exchange and coordination of activities connected to SIS alerts (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation/index_en.htm).

[144] See http://www.nationalcrimeagency.gov.uk/publications/european-arrest-warrant-statistics

[145] See http://www.nationalcrimeagency.gov.uk/publications. Note in this connection the final sentence of paragraph 312 above.

[146] 2008/615/JHA and 2008/616/JHA

[147] (at paragraphs 308-309)

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." [148]

I indicated in my 2014 Report that I would continue to take an active interest in the work that was underway in that connection and, in particular, in the terms and conduct of the proposed pilot exercise. That pilot exercise – which began in March of 2015 – involved the searching of approximately 10,000 unsolved UK DNA crime scene profiles against the DNA databases of The Netherlands, Spain, France and Germany and the reciprocal searching of approximately 3000 such profiles from those countries against the DNA profiles of 40,000 individuals who had been convicted of offences in the UK.

316. On 26 November 2015 the Government published by way of a Command Paper a '*Prüm Business and Implementation Case*'[149] which explored various options as regards Prüm and provided details of the nature and upshot of the pilot exercise that is referred to above. In that paper the Government made clear[150] that it considered that *"it would be in the national interest for the UK to seek to rejoin Prüm."* It also suggested[151] that, if Parliament voted to rejoin Prüm, *"the Information Commissioner and Biometrics Commissioner will be responsible for auditing"* the UK's operation of the system.

317. The matter came before Parliament on 8 and 9 December 2015[152] and it was then decided that the UK would rejoin Prüm on the basis that safeguards proposed in the Command Paper will be brought into force. Those safeguards include conditions to the effect:

    i. that only the DNA profiles and fingerprints of persons actually convicted of offences in the UK will be made available for searching by other EU Member States;

    ii. that demographic information about an individual will only be released following a DNA 'hit' if that hit is of a scientific standard equivalent to that required to report a hit to the police domestically in the UK;

    iii. that such information will only be released in respect of a minor if a formal request for mutual legal assistance has been made; and

    iv. that the implementation of the system will be overseen by a Prüm Oversight Group.

Whilst it has been made clear by the Government that the Biometrics Commissioner and the Information Commissioner will have seats on the Oversight Board[153] and that they *"will be*

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

[149] https://www.gov.uk/government/publications/prum-business-and-implementation-case. [A previous version of that document was published on 30 September 2015.]

[150] (at page 7)

[151] (at page 69)

[152] See: http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151208/debtext/151208-0002.htm#15120843000003 and http://www.parliament.uk/business/publications/hansard/lords/by-date/#session=27&year=2015&month= 11&day=8.

involved in the process",[154] the precise nature of my oversight and/or 'auditing' role has yet to be finalised.

318. It was suggested in the 'Prüm Business and Implementation Case'[155] that:

> *"The Prüm application process and the development requirements for the UK solution mean that it would likely be 2017 at the earliest before any UK Prüm connections could be made. Indeed it may be later."*

Whatever the implementation date, I have no doubt that the Prüm mechanism could prove to be an extremely valuable crime-fighting tool.

[153] http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151208/debtext/151208-0002.htm#15120843000003 (at Column 921).

[154] http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151208/debtext/151208-0002.htm#15120843000003 (at Column 957).

[155] (at page 69)

6. OTHER MATTERS

6.1 THE GOVERNMENT'S PROPOSED BIOMETRICS STRATEGY AND THE HOME OFFICE BIOMETRICS PROGRAMME

319. The Government is in the process of developing a Forensic Science Strategy and a Biometrics Strategy and I have attended numerous working groups and other meetings at which aspects of those proposed strategies have been discussed. In relation to the proposed Biometrics Strategy the Government has stated:

> "*The Government recognises the need to develop a strategic approach to the use and retention of biometrics. This approach should recognise that biometrics is fast-changing and provides opportunities for better secure identity verification, better public services, improved public protection and the ability to identify and stop criminals. This should be balanced against safeguarding the rights of the individual from unnecessary intrusion. The Government's biometric strategy and associated policy framework will support an aligned approach on the use and retention of biometrics and how its implementation is governed*."[156]

320. I have also taken an active interest in the project that has for some time been underway to develop and 'rationalise' the delivery of biometric technologies for which the Government, and particularly the Home Office, has responsibility. Among other things, that project, which is known as the Home Office Biometrics (or 'HOB') Programme, contemplates:

- the replacement of the current IDENT1 fingerprint service with a successor service that delivers 'improved biometric capabilities' – including capabilities in respect of other biometric information such as facial images and iris recognition;
- the 'convergence' of that system with the Immigration and Asylum Biometrics System ('IABS') – which contains the fingerprints of visa and asylum applicants; and
- greater interoperability (and thus easier cross-searching) between those and other Government-run databases which contain biometric information – such as those operated by Her Majesty's Passport Office (HMPO) and the Driver and Vehicle Licensing Agency (DVLA).

I have had a number of meetings with those who are responsible for this project and I shall continue to seek updates on its progress.

321. Important governance, regulatory and privacy/civil liberties issues obviously arise in the context of both the proposed Biometrics Strategy and the HOB Programme, not least as regards the retention and use of biometrics other than DNA and fingerprints, and as regards the sharing of biometric information among organs of the state. The Government has observed:

[156] http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/455/455.pdf. See in particular Recommendation 3.

"we of course understand that there are public concerns around the use and retention of biometrics and we will consider how best to undertake public consultation on this issue as our plans progress."[157]

Since those concerns have been fed in the past by a perceived lack of transparency and/or consultation as regards the state's use of biometric systems, I welcome the upcoming publication of that Strategy and the public consultation that will presumably follow it.

322. Finally in this connection it should be noted:

- that as a result of recent developments in forensic genetics it is or soon will be possible for police forces to derive much more information from traces of DNA that are left at crime scenes than has hitherto been the case; and
- that emerging technologies in that field allow, in particular, for increasingly confident predictions to be made about the likely appearance, age and ancestry of the person who left such a trace, about their relatedness to specified third parties and/or about their proneness to certain medical conditions.

Some of the ethical, regulatory and other issues that arise in connection with these new technologies have been discussed at specialist conferences and seminars in recent months.[158] In my view, however, it is important that those issues are soon also addressed by Government and by a wider public. As the House of Commons Select Committee observed in the Report of March 2015 that is referred to at paragraph 341 below: *"We have seen in the past how public trust in emerging technologies may be severely damaged in the absence of full and frank debate."*

6.2 DNA PROFILING AND LOADING PROBLEMS

323. When DNA samples which have been taken from arrestees are submitted by police 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.

324. In my 2014 Report[159] I referred to a 'fibre contamination' issue that had arisen as regards some DNA samples taken by Thames Valley Police and I indicated that I would be looking further into that issue. I have duly done so and am satisfied that the problem affected

[157] See http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/455/455.pdf (Recommendation 5).

[158] e.g. at the 26th Congress of the International Society of Forensic Genetics: http://isfg2015.org/programme/ and at a recent seminar organised by the NDU.

[159] (at paragraphs 310-315)

fewer than 50 cases, that it posed no risk to the integrity of the national database and that no significant difficulties subsist in relation to it.

325. Officials at the NDU have kept me informed of other issues affecting the National DNA Database by means of 'escalation reports'. I have received and considered a number of such reports – all concerning the loading and searching of DNA profiles to and against that database – and I am satisfied that all necessary measures have been taken to resolve the issues that have arisen, to investigate their causes and impact, and to ensure the integrity of the database and of any matches reported.[160]

6.3 FINGERPRINT GOVERNANCE ARRANGEMENTS

GENERALLY

326. In my 2014 Report[161] I explained that, in contrast to the position as regards DNA samples and profiles, governance arrangements as regards the collection and use of fingerprints for forensic purposes are at best opaque and unsatisfactory. I also explained that steps were being taken to address those deficiencies – particularly by a 'Fingerprint Governance Group' which had been set up by the relevant ACPO lead – and that I was hopeful that real progress would soon be made towards resolving "*the uncertainties that currently exist as regards governance and oversight in this area*".

327. Although some progress has been made in relation to those matters since the date of my previous Report, much remains to be done. Relatively recently, however, it has been decided that, rather than establishing an entirely new governance structure to cater for fingerprints which are held by the police, the jurisdiction of the NDNAD Strategy Board should be expanded so as to cover them. Further work will be required before this change can be made, not least because that Board is now a statutory body.

328. Whilst I shall of course keep these 'fingerprint governance' issues under careful review, I am conscious that their final resolution may well have to await the resolution of the wider governance and other issues that arise in connection with the Biometrics Strategy and the HOB Programme.

IDENT1 AND IABS

329. While the 'Unified Collection' on IDENT1 now contains the fingerprints of around 7.8 million individuals, the IABS database contains the fingerprints of around 15.5 million visa applicants and others. As one would expect, there has long been a process whereby it has

[160] As is the case in relation to numerous other matters, I am grateful to officials at the NDU for their help and assistance in this connection.

[161] (at paragraphs 316-319)

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. This is done via the Police Immigration Fingerprint Exchange ('PIFE') interface or the UKvisas interface, depending upon the type of search transaction, and I understand that these processes have made a considerable contribution to the detection of crime and to the protection of UK borders. As was the position last year, I have seen nothing to suggest that there is or has been any impropriety in this cross-checking process.

6.4 ONGOING IMPLEMENTATION OF POFA

330. Until November of 2014 responsibility for the implementation of the 'biometric' provisions of PoFA lay with a board ('the PoFA Implementation Board') which was chaired by a senior Home Office official and on which police and other stakeholders were represented at a senior level. That board was then disbanded and responsibility for the resolution of any ongoing difficulties was passed to a 'Transitionary Working Group' which, notwithstanding the considerable efforts and hands-on expertise of its members, lacks the authority of its predecessor and has in consequence proved much less successful at progressing necessary changes and work.

331. Further thought is now being given to the powers and responsibilities of this Transitionary Working Group and to the ways in which it might more effectively progress the issues which come before it. I shall continue to press for improvements to be made in that connection.

6.5 NORTHERN IRELAND

332. Although my statutory jurisdiction extends to Northern Ireland as regards National Security Determinations, I have no jurisdiction there as regards the retention and use of biometric material for normal policing purposes. Despite this, however, I have been consulted by the Police Service of Northern Ireland not only about matters relating to national security but also about the upcoming implementation of the new PACE retention regime – which is similar but not identical to that introduced by PoFA – that is to apply in Northern Ireland. I have been more than happy to assist the PSNI in that connection.

333. It has been suggested by both the PSNI and by the Department of Justice (Northern Ireland):

- that it would be helpful to have in place an independent mechanism to provide general oversight of the implementation of the new PACE retention regime in Northern Ireland; and
- that it would seem sensible for that role to be undertaken by me on a non-statutory basis (i.e. by the same person who undertakes a similar oversight role in respect of biometric material taken under PACE in England and Wales).

Given that the additional work for my Office would be relatively limited – and provided only that an appropriate agreement for the sharing of any associated costs can be arrived at between the Home Office and the Northern Irish authorities – I see no reason why that arrangement should be unacceptable. I understand that, although the Home Office takes a similar view, it will respond formally to this proposal only after it has had an opportunity to consult with my successor as Biometrics Commissioner.[162]

6.6 ENQUIRIES AND THE PROVISION OF INFORMATION

REQUESTS FOR INFORMATION BY MEMBERS OF THE PUBLIC

334. My Office and I have received numerous enquiries from, or on behalf of, concerned members of the public, usually requesting information about, and/or confirmation of, the destruction or deletion of their DNA samples and biometric records. Whilst it would have been inappropriate for us to provide any form of legal advice to those individuals, in each of those cases we have sought to inform them about the 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, moreover, we have pursued enquiries with third parties and/or we have advised the individuals concerned as to the steps which were available to them to obtain the information or confirmation they sought.

REQUESTS FOR INFORMATION BY THE POLICE

335. We have also received numerous requests for information and advice from police forces, often in the context of 'live' cases. Whilst we have again declined to provide those forces with legal advice, we have responded in detail to each of their enquiries and we have sought to provide them with helpful information and/or guidance. I am, of course, keen to be told by forces of any concerns or practical problems that have arisen in the context of the PoFA regime so that I can, where appropriate, alert others to them and press for their resolution.

FOI REQUESTS

336. Since my appointment I have received 7 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.[163] However, where I have thought it right to do so, I have volunteered all or much of the information sought.

[162] See paragraph 350 below.

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

6.6 RESEARCH

337. In my 2014 Report[164] I made clear that it is in my view highly desirable that proper – and ideally independent – research be conducted into the impact of the retention regime introduced by PoFA, not least so as to inform policymakers and others as to the effectiveness and proportionality of that regime and as to whether or not the relevant 'lines' have been drawn in the right place. Although I have continued to press for such research to be carried out, it seems that none has yet been conducted and that none is planned for the near future. In the Government's response to my earlier Report, however, Lord Bates did observe that "*these provisions will be subject to existing review mechanisms, including post legislative scrutiny which will consider the effectiveness of the legislation within three to five years of the Act receiving Royal Assent*."

338. At paragraphs 107-109 above:

- I have addressed the issue of post-legislative scrutiny in the context of the provisions of PoFA which allow for the normal retention periods which apply to those who have never been convicted to be extended at the discretion of the Biometrics Commissioner or a District judge; and
- I have suggested that such scrutiny should be informed by proper research.

I take a similar view as regards any post-legislative scrutiny of PoFA more generally and will continue to press for appropriate research to be conducted.

[164] (at paragraphs 332-335)

7. CUSTODY PHOTOGRAPHS AND FACIAL RECOGNITION TECHNOLOGY

339. Although my statutory responsibilities as Biometrics Commissioner relate (like the relevant provisions of PoFA) only to DNA and fingerprints, at paragraphs 336-344 of my 2014 Report I drew attention to developments affecting the retention and use by the police of the third piece of biometric information that is taken from virtually everyone who is arrested for a recordable offence i.e. a facial image or 'custody photograph'. In particular I explained:

    i. that in early April of 2014 I had been informed that "*some 12 million custody photographs had been uploaded to the PND*[165] *and that an automated searching mechanism had 'gone live' five days previously*"; and

    ii. that shortly thereafter I had written to the chair of the relevant working group to express my concerns as to whether, among other things, it could 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 … .*"[166]

340. Between April and November of 2014 I actively pursued my concerns about those developments with senior Home Office officials and with others. Despite doing so, however, by the time of my 2014 Report I had seen little to suggest that significant progress had been made in relation to any of them. As I made clear in that Report,[167] it seemed to me that the then position was:

- "*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,*[168] *it seems likely that many of those images should no longer be being held by the police;*
- *that the uploaded [custody] images are being subjected to a searching mechanism – of, at best, questionable efficiency – whereby [other] 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*

[165] i.e. the Police National Database

[166] (at paragraphs 337-338)

[167] (at paragraph 340)

[168] [2012] EWHC 1681 (Admin)

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.*"

341. As well as raising my concerns about these matters in my 2014 Report, I also raised them in written and oral evidence which I submitted to an inquiry by the House of Commons Science and Technology Committee into *'Current and future uses of biometric data and technologies*'.[169] In a report published in March of 2015[170] that Committee made clear that it shared many of those concerns and it made various recommendations in relation to them. One of those recommendations[171] was "*that the statutory responsibilities of the Biometrics Commissioner be extended to cover, at a minimum, the police use and retention of facial images*". Even before that report had been published, moreover, the relevant Minister had announced that the Home Office would be carrying out a review into the police's retention and use of custody images and the use of facial recognition technology in that connection.

342. I have continued to take an active interest in the work that is being done in relation to the police's retention and use of custody (and other facial) images and I have attended, and spoken at, numerous meetings and conferences at which those matters have been discussed.[172] I have also had some – albeit limited – input into the Home Office review which is referred to above[173] and into a broadly similar review that is being conducted by HMICS[174] into "*Police Scotland's Use of the Facial Search capabilities within the UK Police National Database (PND)*." Like the UK-wide media, the Scottish media picked up on some of the concerns which I expressed in my 2014 Report and the HMICS review was set up following questions about them in the Scottish Parliament.

343. Although it is now some 18 months since I first raised those concerns with the police and with Home Office officials, the position 'on the ground' appears to remain much as it was when I submitted my 2014 Report. In particular, the upshot of the Home Office review has yet to be published and it is my impression that, in the absence of any clear 'steer' from the Home Office:

---

[169] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/current-and-future-uses-of-biometric-data-and-technologies/written/12944.pdf

[170] http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf

[171] i.e. at paragraph 105

[172] I have also visited Leicestershire Police and discussed with them their application of different AFR technology to a local database of facial images and in the context of the 2015 Download Music Festival: see e.g. http://www.bbc.co.uk/news/uk-england-leicestershire-28307938 and http://www.itv.com/news/2015-06-13/download-festival-police-use-facial-recognition-technology-on-revellers/

[173] That input took the form of a written response to a 'Consultation Document' which was sent to me (and others) by the review team on 9 July 2015.

[174] i.e. Her Majesty's Inspector of Constabulary in Scotland

- police forces in England and Wales have continued to upload custody images to the PND regardless of whether the individuals in question have or have not been convicted of, or even charged with, an offence;
- all the custody photographs on the PND have continued to be searched against by forces using facial recognition software; and
- few if any steps have been taken to remove from that database the custody photographs which, in the light of the judgment in *R (RMC and FJ) v MPS*, it seems likely that the police should no longer be retaining.[175]

I see no reason to believe that that situation will quickly change even after the results of the Home Office review are published.[176]

344. I am concerned at the absence of any substantial progress in relation to these matters. Among other things – and as I have repeatedly made clear – I am concerned that the considerable benefits that could be derived from the searching of custody images on the PND may be counterbalanced by a lack of public confidence in the way in which the process is operated, by challenges to its lawfulness and by fears of 'function creep'. As I have pointed out above, similar – but even more difficult – issues seem almost certain to arise in the near future in connection with the wider sharing of biometric information among organs of the state and the automated searching of other Government-run databases.[177] My hope is that those issues will be addressed with a rather greater degree of urgency.[178]

[175] I also understand that the retention of custody photographs by the police continues to be an issue in 6 applications that have been made to the ECtHR.

[176] I understand that the situation as regards Police Scotland's use of PND facial searching technology is rather different. It seems that Police Scotland only ever upload custody photographs to the PND in circumstances where the individuals in question have been charged, and that they purge from that database the photographs of those who are subsequently acquitted and have no other convictions. I further understand that facial recognition technology is not applied to any local database of custody photographs that is held by Police Scotland.

[177] See paragraphs 320-321 above and the obvious possibility that the police will soon want to access – and to institute automated searches of – the much larger databases of facial images that are held by HMPO and the DVLA.

[178] I note that at paragraph 101 of the Select Committee Report to which I referred at paragraph 341 above, the Committee emphasised the desirability of avoiding *"a biometric application once again being put into operational use in the absence of a robust governance regime"*.

8. RESOURCES ETC.

8.1 STAFFING

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

- a Head of Office;[179]
- a Policy and Casework Manager; and
- a Caseworker.

As is mentioned above, although each of them is a Home Office employee, they work under my direction and I am satisfied that they operate entirely independently of outside pressure. 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 am satisfied 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, a Home Office recruitment freeze has until recently prevented me from filling that post. In September of this year I was informed that the position as regards recruitment by NDPBs sponsored by the Office of Security and Counter Terrorism, of which my Office is one, has now been relaxed and I will therefore shortly be embarking on a recruitment exercise to fill this longstanding vacancy.

8.2 BUDGETS AND EXPENDITURE

347. My Office's budget for the financial year 2014/15 was £300,000. For a number of reasons – including in particular the recruitment freeze which is referred to above and the fact that, since January of 2015, my former Policy and Casework Manager has been 'acting-up' as my Head of Office – I underspent that budget by some £37,000.

348. After various meetings and exchanges of correspondence with officials from my sponsoring departments within the Home Office it has now been agreed that my Office's budget for 2015/16 will remain at £300,000. It seems likely that, for much the same reasons as previously, that budget will again be underspent.

[179] This position is currently filled on a temporary basis.

8.3 ACCOMMODATION AND WEB PRESENCE

349. 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 my 2014 Report[180] I expressed concerns about aspects of my web presence and of the accommodation for my Office which seemed to me unsatisfactory in view of, among other things, my need for perceived as well as actual independence. Since that time nothing of substance has changed as regards those matters and I shall continue to keep them under review.

8.4 EXPIRY OF TERM OF APPOINTMENT

350. My appointment as Biometrics Commissioner was for a three-year term which will expire in March of 2016. Although I have not sought to extend that term, I have made clear that I am, if necessary, willing to stay in post for somewhat longer to allow for a smooth takeover by my successor.

351. I am very grateful indeed to all those who have assisted me in my work and, in particular, to my colleagues at the OBC. If they are even half as helpful, good-humoured and patient with my successor as they have been with me, he or she will be fortunate indeed.

[180] (at paragraphs 354-359)

LIST OF ACRONYMS

ABH	Actual Bodily Harm
ACPO	Association of Chief Police Officers (now known as the National Police Chiefs' Council ('NPCC')
ACRO	Association of Chief Police Officers Criminal Records Office
BRU	Biometric Retention Unit
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CTA	Counter-Terrorism Act 2008
CTFS	Counter Terrorism Forensic Services (now known as Secure Operations – Forensic Services)
EAW	European Arrest Warrant
ECtHR	European Court of Human Rights
EMSOU-FS	East Midlands Special Operations Unit – Forensic Services
FOI request	A request under the Freedom of Information Act 2000
FSPs	Forensic Service Providers
GBH	Grievous Bodily Harm
GDS	Government Digital Service
GMP	Greater Manchester Police
HMIC	Her Majesty's Inspectorate of Constabulary (England and Wales)
HMICS	Her Majesty's Inspectorate of Constabulary in Scotland
HMPO	Her Majesty's Passport Office
HOB	Home Office Biometrics Programme
IABS	Immigration and Asylum Biometric System
IDENT1	The national police fingerprint database
JCHR	Joint Committee on Human Rights
JFIT	Joint Forensic Intelligence Team
JSIU	Joint Scientific Investigation Unit

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
NPCC	National Police Chiefs' Council (formerly known as the Association of Chief Police Officers ('ACPO')
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
SOFS	Secure Operations – Forensic Services (formerly known as Counter Terrorism Forensic Services ('CTFS')
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
UKICB	United Kingdom International Crime Bureau

ISBN 978-1-4741-2935-0