ANNUAL REPORT 2017

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Paul Wiles

March 2018

Office of the Biometrics Commissioner

ANNUAL REPORT 2017

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.

June 2018

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

Any enquiries regarding this publication should be sent to us at enquiries@biometricscommissioner.gsi.gov.uk

ISBN 978-1-5286-0370-6

CCS0518559084 06/18

Printed on paper containing 75% recycled fibre content minimum

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

FOREWORD

This is the fourth Report by the Commissioner for the Retention and Use of Biometric Material. I am the second Commissioner to hold that office and was appointed by the Home Secretary in June 2016.

This Report was finished and sent to Ministers on the 26th March 2018.

In order to make this Report as easy for the general reader as possible I have avoided detailed references to the various legal provisions of the Protection of Freedoms Act 2012 (PoFA) which created my role and the requirement for an Annual Report. Where such reference is unavoidable I have tried to be brief or to place the material in an appendix. More details on the legal provisions contained in PoFA can be found in the first two Annual Reports.

My Office should consist of four staff to help me deal with my casework functions and the programme of inspection visits and meeting attendance necessary for the production of this Report. I have never had four staff working in my Office since my appointment. Indeed, for the last few months, I have only had one member of staff. Without the extraordinary dedication of my former Head of Office, Gemma Gyles, and my present Head of Office, Lucy Bradshaw-Murrow, who during those months have been my only staff, this Report would never have been completed on time. However, by giving priority to producing a report for the Home Secretary other work has fallen behind, such as the section 63G casework and the investigation of new, emerging problems.

Some new staff will be joining me shortly and once they are trained it must be a priority to catch up with those other issues. The casework would have fallen even further behind if two other colleagues, Jim McAVeety and Aradhna Jaswal, who left during the year, had not ensured that it was up to date at the point when they left. To all of my colleagues during the year I owe a very real debt of gratitude for their professionalism and unfailing good humour in spite of the pressures they had to cope with.

Paul Wiles

2018

CONTENTS

1. INTRODUCTION

1.1 WHAT DOES THE BIOMETRICS COMMISSIONER DO?

1. The position of Commissioner for the Retention and Use of Biometric Material ('Biometrics Commissioner') was created by the Protection of Freedoms Act 2012 to provide assurance to the Home Secretary and to Parliament on the working of that legislation. In addition, that legislation granted to the Biometrics Commissioner oversight and some limited decision making powers as regards the retention and use of biometrics (DNA samples, DNA profiles and fingerprints). For the oversight of the retention and use of biometrics in matters of national security the Commissioner's remit is UK wide[1] but for other criminal matters the remit is for England and Wales only.

2. This is the fourth Annual Report of the Biometrics Commissioner.[2]

3. The Protection of Freedoms Act (PoFA) is the legislation which currently governs the police use of biometrics and was passed in response to a court judgment which held that previous legislation was not proportionate in the way in which it balanced the public interest in the police use of biometrics and the individual's right to privacy.[3] The new proportionality put in place by PoFA is, like all legislation, itself open to further challenge in the courts.

4. PoFA governs police use of fingerprints and DNA, which were the two biometrics then used by the police.[4] Since PoFA was passed there has been a very rapid growth in the availability and utility of other biometric technologies. Digital facial images are already routinely collected and stored by the police and they are experimenting with facial image matching in public places. Other technologies, such as voice recognition, are also being trialled by the police and a wider set of biometrics are being deployed by the private sector and to a limited extent elsewhere in government. None of these second generation biometrics are covered by PoFA and their deployment has run ahead of governance arrangements and legislation. This issue is discussed further in Chapter 8 of this Report.

5. The Biometrics Commissioner is required to provide an annual report to the Home Secretary. The Home Secretary may, after consultation with the Commissioner, exclude

---

[1] See further Chapter 5 of this Report.

[2] The publication of the last two Reports was significantly delayed due to, amongst other reasons, the calling of elections. The result of these delays is that the timing of the Reports have varied and so, therefore, have the periods they have reported on.

[3] 2008 the Grand Chamber of the European Court of Human Rights (ECtHR) in *S and Marper v United Kingdom* 2008) 48 EHRR 1169. For a more detailed discussion of the process that led to the passing of PoFA see the Annual Report of the Biometrics Commissioner, 2016, Section 1.2.

[4] In addition, PoFA also governs the use of footwear prints which, though not a biometric, was the other personal forensic for which the police at the time maintained a database.

from publication any part that they consider would be contrary to the public interest or prejudicial to national security.[5] No such exclusions have been made to this report or any previous report.

1.3 USE OF BIOMETRICS BY THE POLICE

6. Different biometrics provide different evidential support that any claimed match is true. For this reason their quality and evidential use in the criminal justice process needs to be carefully judged and that process is overseen by the Forensic Science Regulator, Dr Gillian Tully.[6] The result is that fingerprints and DNA are both used and accepted extensively in the criminal justice system in England and Wales. It is unusual for such biometric evidence to be challenged in court, except where the trace material is very incomplete and/or from multiple individuals. This position has not yet been achieved for second generation biometrics or even some new technologies being introduced for DNA or fingerprints.

1.4 PRESENTING BIOMETRIC EVIDENCE

7. Biometric evidence is used in court through the presentation of expert evidence and depends on an assessment of the quality and applicability of the underlying science and judgements made on that evidence.

8. This is one of the areas where my remit has some overlap with that of the Forensic Science Regulator and we are working with the Royal Statistical Society (RSS), and others with expertise and experience of criminal justice decision making, to develop and test a standardised means of presenting the quality and strength of forensic evidence to help those involved in criminal justice decision making.

9. The first step in this process is to agree among the scientific community how evidence should be presented, its limitations acknowledged and statistical probabilities expressed. This framework would be used by expert witnesses in giving evidence and be shared with the judiciary to help them judge expert witnesses appearing before them. This stage commenced with a conference in Birmingham in October 2017 and was lead by Dr Tully since it is part of her regulatory remit.

10. Once this first step is agreed we can then examine the basis for helping others in the criminal justice process better understand how forensic evidence should guide decision making, ranging from the police to juries. The intelligibility of such guides could be empirically trialled.

[5] PoFA section 21(5)

[6] See http://www.gov.uk/government/organisations/forensic-science-regulator

11. At the same time a series of guides (primers) for the judiciary on types of forensic evidence that may be presented in court is being produced by scientists and practitioners, approved by the Royal Society and the Royal Society of Edinburgh under judicial chairmanship and under the general oversight of a steering group chaired by Lord Hughes of the Supreme Court. Two such guides have been produced so far on DNA analysis and forensic gait analysis.[7]

[7] https://royalsociety.org/~/media/about-us/programmes/science-and-law/royal-society-forensic-dna-analysis-primer-for-courts.pdf and https://royalsociety.org/~/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf

2. BIOMETRIC DATABASES

2.1 THE GOVERNANCE OF NATIONAL DATABASES

12. The National DNA Database (NDNAD) was overseen by the National DNA Strategy Board (NDNASB), which was given a statutory role in PoFA.[8] It was (and still is in its current iteration) chaired by a representative of the National Police Chiefs' Council (NPCC) and includes representatives of the Home Office and of the Police and Crime Commissioners who are the voting members. Also in attendance as observers are the Chair of the Biometrics and Forensic Ethics Group,[9] the Forensic Science Regulator, the Biometrics Commissioner, the Information Commissioner[10] and representatives of the devolved administrations. Since March 2016, fingerprints and footwear impressions have been added to the remit of the Strategy Board and it has become the Forensic Information National Database Strategy Board (FINDS-SB). FINDS-SB monitors the performance of these databases and their use by the police. It also issues guidance to the police on the use of the databases, including in relation to meeting the requirements of PoFA.

13. The extension of the remit of the Strategy Board is a welcome development since it brings DNA, fingerprints, the counter-terrorism database and footwear impressions (all subject to regulation by PoFA) within a proper, transparent and, moreover, mature national governance structure. There are, however, other police biometric databases that are not within the remit of FINDS-SB, most notably the facial images held on the Police National Database (PND), of which more later.

14. FINDS-SB publishes an annual report which is laid before Parliament[11] and includes data about the operation of the databases. Similar data is included in this report simply to ensure that it is self contained for the reader, although our data is mainly for a calendar year rather than a fiscal year as in the FINDS-SB Report.

15. It will inevitably take time for FINDS-SB to bring these new additions to its remit to the same standard of governance and transparency as already exists for DNA. Eventually this will mean that similar data will be available for both DNA and fingerprint databases but given the complexity of the fingerprint landscape, this will take some time. For that reason the

[8] See section 63AB of Police and Criminal Evidence Act 1984 (PACE) as inserted by section 24 of POFA.

[9] Originally called The National DNA Database Ethics Group but during the year given an extended remit to match that of the Strategy Board and re-named the Biometrics and Forensic Ethics Group – see https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group

[10] See http://www.ico.org.uk/

[11] https://www.gov.uk/government/publications/national-dna-database-annual-report-2015-to-2016

information in this report on the police use of fingerprints is still not of the same standard as that for DNA.

NATIONAL DNA DATABASE

16. The National DNA Database was established in 1995 and, by the end of the calendar year 2017, held 5,617,016 subject DNA profiles for England and Wales. This equates to an estimated 4,887,588 individuals. UK holdings total 6,734,543 subject and crime scene profiles or an estimated 5,344,537 individuals out of a population of 65,648,100 (roughly 10% of those beyond the age of criminal responsibility).[12] The number of DNA subject profiles added to the database has declined as a result of the fall in police recorded crime, and/or the number of persistent offenders being rearrested, from 540,100 profiles added in 2009/10 to 269,500 in 2016/2017.[13]

TABLE 01: Number of DNA profiles held (year ending 31 December 2017)

	Subject profiles	Crime Scene profiles	Total
England & Wales[14]	5,617,016	551,175	6,168,191
Rest of UK[15]	534,577	31,775	566,352
Total	**6,151,593**	**582,950**	**6,734,543**

(Source: FINDS-DNA[16])

[12] ONS: Population Estimates for UK, England and Wales, Scotland and Northern Ireland: Mid-2016, June 2017. The percentage is an estimate since the age of criminal responsibility varies across the UK.

[13] Data supplied by FINDS-DNA.

[14] Includes British Transport Police

[15] Includes Scotland, Northern Ireland, Isle of Man, Channel Islands and Customs and Excise.

[16] Special thanks to Kirsty Faulkner and Caroline Goryll of FINDS-DNA for their help in preparing the relevant data.

TABLE 02: Total DNA Holdings on NDNAD by Profile Type (year ending 31 December 2017)

	Arrestee	Volunteer[17]	Crime-scene from mixtures[18]	Crime-scene non-mixtures	Unmatched Crime-scenes[19]
England & Wales	5,615,005	2,011	78,836	472,339	182,023
Rest of UK	532,410	2,167	1,434	30,341	16,648
Total	**6,147,415**	**4,178**	**80,270**	**502,680**	**198,671**

(Source: FINDS-DNA)

The significant increase in crime scene stains involving mixtures of more than one person's DNA (up from 55,429 to 80,270) reflects the increasing ability claimed by forensic scientists to analyse such complex stains.

NATIONAL FINGERPRINT DATABASE: IDENT1

17. The National Automated Fingerprints Identification System (NAFIS) became fully operational in 2001. NAFIS held all fingerprint sets (tenprints) taken from persons arrested in England and Wales. Tenprints obtained from offenders convicted of certain serious offences in Scotland and Northern Ireland were also added to NAFIS. NAFIS provided the opportunity to search unidentified finger-marks retrieved from crime scenes against tenprints obtained from arrested persons. Livescan[20] came into operation in 2002 and has recently been updated as part of the Home Office's Biometrics Programme (HOB). NAFIS was succeeded by IDENT1 in 2004 which enabled the storage and search of arrestee palm prints and unidentified palm marks from scenes of crime. In 2007 Scotland began enrolling tenprints obtained for arrests in Scotland to IDENT1 and in 2013 Northern Ireland began enrolling tenprints obtained for arrests in Northern Ireland to IDENT1. Presently, fingerprints taken under PACE or its equivalent in the UK are enrolled onto IDENT1 for storage and search.

[17] 'Volunteer' profiles include a limited number of those given voluntarily by vulnerable people at risk of harm and which are searchable on the NDNAD, convicted persons and/or sex offenders.

[18] Mixed profiles include the DNA information of two or more persons.

[19] The number of unmatched crime scenes is included in the crime scene from mixtures and non-mixtures figures.

[20] Livescan is an electronic fingerprint capture system for capturing subject fingerprint and palm print data for enrolment onto the database

TABLE 03: Number of fingerprints held on IDENT 1 for all forces (year ending 31 December 2017)

Subject Records	Arrest Ten-Print Fingerprints[21]
8,093,575	24,682,309

(Source: FINDS - National Fingerprint Office in consultation with the IDENT1 supplier)

TABLE 04: Total Holdings on IDENT1 by classification (year ending 31 December 2017)

Pseudo Sets[22]	Unmatched Crime Scene Finger-marks	Unmatched Crime Scene palm marks	No of Cases with Unidentified Crime marks	Cases in Serious Crime Cache (SCC)
5,508	1,937,874[23]	359,895[24]	981,806[25]	1,173

(Source: FINDS - National Fingerprint Office in consultation with the IDENT1 supplier)

2.2 THE USE OF THE DATABASES

NATIONAL DNA DATABASE

ADDITIONS TO THE NDNAD IN 2017

18. The National DNA Database as of the year ending 31 December 2017, held 6,151,593 subject profile records and 582,950 crime scene profile records. In 2017, 261,962 new subject profiles were added to the database, and 41,577 crime scene profiles were also added to the database (See Table 05 below).

[21] Taken under PACE or equivalent (also includes Pseudo sets – see Table 04 below).

[22] 'Pseudo sets' include records for individuals believed to be at risk of harm, e.g. those at risk of exploitation or honour based violence.

[23] 3,232 unmatched finger-marks in the Serious Crime Cache and 1,934,642 unmatched finger-marks from the unidentified marks database (non SCC).

[24] 793 unmatched palm marks in the Serious Crime Cache and 359,102 unmatched palm marks from the unidentified marks database (non SCC).

[25] 1,173 SCC cases and 980,633 cases in the unidentified marks database.

TABLE 05: Additions to the NDNAD (year ending 31 December 2017)

	Arrestee[26]	Volunteer[27]	Crime-scene from mixtures[28]	Crime-scene non-mixtures
England & Wales	225,625	1	26,056	13,921
Rest of UK	36,334	2	381	1,219
Total	261,959	3	26,437	15,140

(Source: FINDS-DNA)

19. The number of profiles held on the National DNA Database reached a peak of 6.97 million in the **fiscal** year 2011/12, declined to 5.63 million in 2012/13[29] and then increased to its present level of 6.02 million; this is because the number of new profiles loaded has declined from 540,100 in the fiscal year 2009/10 to 269,489 in 2016/17. The number of crime scene profiles loaded onto the database has declined from 50,000 in 2008/09 to 40,829 in the fiscal year 2016/17.

20. In the fiscal year 2016/17, 165,874 subject profile records were deleted from the database[30] and 5,004 crime scene profile records were deleted.[31]

MATCH RATES

21. The extent to which crime scenes are examined for DNA stains varies significantly between offence types.[32] This is because the possibility that DNA is likely to be found at a crime scene varies by offence and, in addition, more serious incidents are likely to be prioritised.

[26] The figures in the equivalent column in last year's Annual Report were incorrect and badly inflated the numbers of arrestees.

[27] 'Volunteer' profiles include those given voluntarily by vulnerable people at risk of harm, convicted persons or sex offenders.

[28] Mixed profiles include the DNA information of two or more persons.

[29] This was in part due to deletions required by the newly enacted PoFA legislation.

[30] Including 106 under the 'Deletion of Records from National Police Systems' Guidance; see also Section 6.3 below.

[31] All these fiscal year figures are provided by FINDS-DNA. Comparative figures are not available for calendar years.

[32] Source: FINDS-DNA.

22. Given that most of those convicted of a recordable offence will have their DNA and fingerprints retained,[33] biometrics will be available to police investigators for most of those who reoffend. Repeat offenders make up a significant proportion of overall offending. As a result the rate at which crime scene profiles produce a match to subject profiles held on the database is high (presently 66.5% for England and Wales in 2017 which is fractionally lower than last year).

TABLE 06: Match Rate for Matches obtained immediately on loading for England and Wales Forces (year ending 31 December 2017)[34]

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	**40,233**	**225,625**
No. of Matches	26,764 (66.5%)	4,662 (2.1%)

(Source: FINDS-DNA)

TABLE 07: Match Rate for Matches obtained immediately on loading for all UK forces (year ending 31 December 2017)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	**41,577**	**261,964**
No. of Matches	27,260 (65.6%)	5,178 (2.0%)

(Source: FINDS-DNA)

23. FINDS-DNA have not been collating data for the inter-country match rates within the UK (i.e. matches between England and Wales, Scotland and Northern Ireland) but the rates given in last year's Report are unlikely to have changed significantly in such a short period.

ATTRITION RATES

24. The data and comments in last year's Report about the attrition rate from recorded crime to outcome involving DNA is not repeated this year because such rates will not have changed significantly in such a short period. Those interested should refer to Table 09 in last year's Report at page 11.

[33] Whilst PoFA would allow all such biometrics to be retained, biometrics are not necessarily taken in all such cases.

[34] Figures do not include profiles which were loaded and deleted in the same month as these are not currently recorded by the NDNAD in their Management Information.

ERROR RATES

25. Police forces and Forensic Service Providers (FSPs) have a number of safeguards in place to prevent and identify errors in the processing and interpretation of DNA samples. Moreover, FINDS carry out daily integrity checks on the DNA profile records that are loaded onto the NDNAD. Error rates[35] that are found in the processing of DNA are generally acceptable, for example sampling and record handling errors by FSPs are made in relation to fewer than 0.001% of subject profiles. Errors are made by FSPs when interpreting subject profiles in fewer than 0.002% of cases and in interpreting DNA profiles from crime-scenes in relation to around 0.1%. [36]

26. Since April 2016, FINDS-DNA have collected data on errors in DNA sampling by police forces, both at crime-scenes and in custody. This data is provided to FINDS-DNA by the relevant police forces. The majority of police forces have now responded to requests for data but seven forces have still failed to provide the data for their force[37]. This is worrying since they have failed to do so for 2 years and one would expect forces that have adequate governance processes to be able to provide such data. The data collected has not yet been fully verified given that the data set is not complete and work is still being done, for example to judiciously categorise errors, therefore further work is required before conclusions can be drawn. It is clear, however, from the data that is available, that errors found when subjects' DNA samples are taken sometimes appear to be unacceptably high and to vary significantly by force. The FINDS-SB has identified this problem as in need of urgent improvement and is planning to issue guidance on sampling. It is reassuring to note that the majority of these errors are identified either by forces themselves before submission of the sample to the FSPs or by the FSPs when processing the sample. Nevertheless, integrity monitoring by FINDS does discover a small number of force handling errors on the NDNAD[38]. These errors occur in an average of around 0.04% of all subject profiles loaded to the NDNAD.

27. Sample or record handling errors by police forces made when taking subjects' DNA samples have potential implications for the future detection of crime as where a sample cannot be submitted and/or profiled due to an error, and a replacement sample is not taken from the subject, the potentially important DNA data is lost.[39] On my visits to police forces I have found that procedures for re-sampling vary widely; some forces have defined processes for

[35] (i.e. the number of errors found through the DNA supply chain from sampling to matching against the NDNAD)

[36] Source: FINDS-DNA.

[37] Avon and Somerset, City Of London, North Wales, Northumbria, Staffordshire, Warwickshire and Wiltshire.

[38] These occur when the DNA profile is associated with the wrong information.

[39] At the very least additional police resources are needed to re-take the sample from the subject (who may well have left police custody).

reporting failed samples and ensuring that the sample is re-taken, some forces only re-take samples in relation to certain, more serious offences and others have no follow-up process at all beyond reporting the error to the officer in the case. It is therefore difficult to quantify the extent of DNA data losses arising from sampling or handling errors, even amongst forces who have reported their error rates to FINDS-DNA.

28. Of particular concern are the, admittedly very small number (0.04%), of cases where a data handling error is not identified until FINDS integrity checks on the NDNAD. Errors on the NDNAD have the potential to affect NDNAD matching, i.e. the profile/record allows for missed matches, mismatch or elimination to occur. Were these errors not to be identified there is a chance, albeit a very small one, of a miscarriage of justice. Whilst it is important to acknowledge these risks, it is reassuring that FINDS-DNA have such rigorous processes for checking and identifying errors in the DNA data that they receive.

NATIONAL FINGERPRINT DATABASE: IDENT1

ADDITIONS TO IDENT1 IN 2017

29. IDENT1, as at 31 December 2017, held 8,093,575 unique arrestee subject tenprint records, 937,874 unmatched finger-marks and 359,895 unmatched palm marks relating to 981,806 cases of unidentified scenes of crime marks. During 2017, 105,896 unique subject records and 42,819 crime scene cases were added to the database (See Table 10 below).[40]

TABLE 10: Additions to the Database (year ending 31 December 2017)

Arrest Records	Subject Ten-print Fingerprints	Cases with Unidentified Crime Scene Marks[41]	Number of Unidentified marks in the Serious Crime Cache[42]
105,896[43]	910,251	42,819	342

(Source: FINDS - National Fingerprint Office in consultation with the IDENT1 supplier)

30. During 2017, 3,537 PACE subject records were deleted from the database.[44] Deletions occur when retention rules mean that the record should no longer be maintained. This process is

[40] The quoted figures represent the net increase in records held on IDENT1 accounting for the overall difference of records added and deleted during 2017. If making a comparison with my previous Annual Report note that figures were not available for the whole of 2016 due to the new reporting regime.

[41] Figure provided refers to the number of cases. Cases may have multiple marks attributed to them.

[42] Figure is for number of marks not cases as this data is not available.

[43] This figure shows the overall increase in unique PACE records on IDENT1, accounting for new persons created and deleted during the period.

[44] Comparative figures on deletions for crime-scene marks are not available.

largely automated as the PNC stores the retention rules and initiates deletion messages to IDENT1 accordingly.

MATCH RATES

31. The match rate for fingerprints and palm prints, compared to that for DNA, is currently difficult to calculate in a meaningful manner since the data available to us is basically contract compliance data and not designed for this purpose. Nevertheless, match rate ratios are now published by the National Fingerprint Office on a monthly basis. The ratios are the number of searches performed for each (1) declared identification.

TABLE 11: Fingerprint identification ratios (2017)

	Identification ratio for December 2017	Identification rates for each month of 2017 as an average
Scene of crime palm mark to palm print	21.31	16.93
Scene of crime fingermark to tenprint	26.06	20.33
Tenprint to scene of crime mark	134.04	143.35

(Source: FINDS - National Fingerprint Office in consultation with the IDENT1 supplier)

32. The way fingerprints are searched and used by the police, however, is different from their use of DNA. Fingerprints are much cheaper to process and use than DNA. The automated search function provided by Livescan machines, which communicate directly with IDENT1, allow ten-print sets to be immediately searched against one or more collections of fingerprints on that database, including the cache containing unidentified crime-scene marks. For these reasons the police say that fingerprints are of greater investigative value and, initially at least, the prime biometric used to check identity. In police custody suites, fingerprints are taken from every arrestee and used to verify the identity of the subject whereas DNA samples are often only taken where the subject's DNA profile is not already on the NDNAD.[45]

2.3 KNOWLEDGE BASE ON BIOMETRIC USE EFFECTIVENESS

33. I commented last year that a knowledge base on the use effectiveness of both DNA and fingerprints in police investigation does not exist, in part because it is very difficult to

[45] DNA samples are usually re-taken in custody in relation to major crimes or where an existing DNA profile has been obtained using SGM or SGM plus chemistries and the profile already held may require upgrading using the current DNA-17 profiling method. See further *National DNA Database Strategy Board Annual Report 2015/16* at paragraph 1.5.1.

identify the added value from the biometrics compared to other information.[46] The same point has been made by others and as part of the police's Transforming Forensics Programme[47] an attempt is now being made to quantify the benefits of biometrics used by the police. Such an analysis will not be easy but it is necessary as the basis for future decision making about which biometrics should be deployed by the police.

34. With the emergence of second generation biometrics in UK policing, such as the large scale existing use of facial images but also the experiments with other biometrics, the need to understand the cost effectiveness of different biometrics is becoming ever more important. In future the police may have available to them a choice of a larger number of biometrics than presently. However, to be effective each biometric will need a database and it is unlikely that the police will be able to afford to routinely, operationally use and maintain a national database for all of the biometrics available. Furthermore, one might expect the marginal value outcome to decline as the number of biometrics used increases. To guide their choices the police will need to understand the relative utility and cost effectiveness of each biometric. Chief Constable Debbie Simpson, the NPCC lead on biometrics, has identified this as an important future need for the police.

[46] Commissioner for the Retention and Use of Biometric Material: *Annual Report 2016*, Section 2.4.

[47] See: http://www.apccs.police.uk/police-reform/specialist-capabilities/

3. BIOMETRIC RETENTION AND POFA COMPLIANCE

3.1 THE BIOMETRIC REGIME INTRODUCED BY POFA

35. What Parliament decided when it introduced the PofA regime was:

- that as regards the retention of biometric material by the Police, much more restrictive rules should apply to the retention of DNA samples than to DNA profiles and fingerprints;
- that the rules applying to DNA profiles and fingerprints should draw a clear distinction between individuals who have been convicted of an offence and those who have not; and
- that a similar, yet less prescriptive retention regime, should also apply to footwear impressions.

That new regime – which was largely introduced by way of amendments to the Police and Criminal Evidence Act 1984 (PACE) – is summarised in general terms below.

FINGERPRINTS AND DNA

36. In respect of the police use of biometrics, the provisions in PoFA only provide a framework for the retention and use of fingerprints, DNA samples and DNA profiles. There is presently no legislation which applies similar principles to other biometrics used by the police – for a further discussion of this see Chapter 8.

37. Although the police have been taking fingerprints for over 100 years as paper-based ink set records, they are now commonly taken digitally and loaded to the National Fingerprint Database (IDENT1). Fingerprints can be matched automatically, having been taken on a scanner (known as a Livescan machine) using matching software, although there is still an important role for fingerprint experts in checking potential matches.

38. DNA samples are mainly taken by way of mouth swabs from which a DNA profile is derived by laboratory analysis.

39. DNA profiles derived from DNA samples taken from arrestees are loaded onto the National DNA Database (NDNAD).

SUMMARY OF POFA RETENTION RULES

40. For fingerprints, DNA samples and DNA profiles taken by the police there are clear rules as to when biometrics can be retained and for how long. The general rule is:

- that any DNA sample 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 taken;[48]
- that if an individual is convicted of a recordable offence their biometrics (DNA profile and/or fingerprints) may be kept 'indefinitely';
- that if an individual is charged but not convicted for certain more serious offences (called 'qualifying offences'[49]) then their biometrics (DNA profile and/or fingerprints) may be retained for three years; and
- that if an individual is arrested for but not charged with a qualifying offence an application may be made to the Biometrics Commissioner for consent to retain the DNA profile and/or fingerprints for a period of three years from the date that person was arrested.

There are, however, a number of exceptions and more detailed qualifications to these general rules relating to the age of the arrestee, the offence type and on grounds of National Security. These are set out fully in **Appendix A** and summarised in the tables below.

TABLE 11: PoFA Biometric Retention Rules

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** **1st conviction – sentence over 5 years** **2nd conviction**	**Length of sentence + 5 years** **Indefinite** **Indefinite**

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

[49] See section 65A(2) of PACE. A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.

Non convictions

Alleged offence	Police action	Time period
All Offences	**Retention allowed until the conclusion of the relevant investigation[50] 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	**Penalty Notice for Disorder (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)[51]**

THE MEANING OF 'INDEFINITE' RETENTION

41. There has been some debate and disagreement as to what 'indefinite' biometric retention, under sections 3 and 5 [52]of PoFA, means in practice.

42. The plain meaning would be that the biometrics may be retained forever. Whilst this is a simple concept to employ, over time the limitless retention of records would inevitably clog the databases with biometrics of no further utility at increasing expense to the tax-payer and this was probably not what Parliament intended.

43. The Home Office's Biometrics and Forensics Ethics Group has recommended to the Home Office that 'indefinite retention' should in practice mean retention until the person reaches 100 years of age.[53] They recommend such a retention period should apply to retention of fingerprints and DNA, under PoFA, but also to custody images which are governed by MOPI

[50] For detailed discussion of the definition and operational application of *"conclusion of the investigation",* see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at paragraphs 25-28.

[51] Following initial retention period allowed for by terrorism legislation – see Annex C

[52] Which amend sections 63F and 63I of PACE.

[53]See: https://www.gov.uk/government/publications/ethical-advice-on-the-retention-of-biometrics-from-convicted-persons

(Management of Police Information) rules drawn up by the College of Policing.[54] Even then, records can potentially be retained if there is still an open investigation involving the subject. This is also the solution adopted in Scotland. The Ethics Group also recommend different, shorter, retention rules for those *"convicted, at a relatively young age (but above 18 years of age), of offences which, whilst relatively minor offences, are sufficiently serious to allow for their biometrics to be retained indefinitely under current legislation"*.[55] That change, however, would require amendment of primary legislation (PoFA).

44. We await the Home Office's response to this recommendation.

FOOTWEAR IMPRESSIONS

45. Footwear impressions are not a biometric but nevertheless they are included in PoFA. Section 15 of PoFA[56] provides that:

> *"Impressions of footwear may be retained for as long as is necessary for the purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of prosecution."*[57]

46. Presently there are two national databases of footwear impressions: the National Footwear Reference Collection (NFRC), which contains shoe impressions taken from arrested persons and the National Footwear Database (NFD) which contains footwear marks recovered from crime scenes. Both databases are currently administered by FINDS-DNA and images are retained indefinitely. Impressions on the NFRC are held in anonymised form with each impression allocated a unique reference code. It is therefore not possible to determine from the database image alone who the footwear impression belongs to or the offence/arrest event in connection with which it was taken.

47. I reported last year that it was not clear to me how the PoFA retention rules were being applied in practice nor what use was being made of the national databases. I therefore wrote to Chief Constables asking for a copy of their policy as regards the retention and use of footwear impressions.

48. The replies to my letter show that there is not an agreed national policy or even approach being applied to the retention of footwear impressions by all police forces in England and Wales. Indeed, not all forces routinely collect footwear impressions. Some routinely take impressions at custody suites, such as the MPS with their Treadware scanner system, but

[54] See: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#custody-images

[55] https://www.gov.uk/government/publications/ethical-advice-on-the-retention-of-biometrics-from-convicted-persons

[56] Which amends section 63F of PACE.

[57] See: http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/1/enacted.

others only take impressions on a casework basis. The length of time for which footwear impressions are retained also varies and whilst 12 months is common, force practice varies from keeping impressions for 6 months to indefinite retention. Some forces upload their impressions onto the national databases but many do not.

49. Footwear impressions are not a biometric and the utility of subject's footwear impressions is short-lived since shoes will wear over time and the impressions they leave will inevitably change. I was therefore puzzled to learn that impressions are not deleted from the NFRC, but are held indefinitely for reference purposes[58].

50. There is no national data available on the use made of footwear impressions and the outcomes. FINDS-DNA are examining policy with regards to the footwear impressions databases but that leaves wider policy questions about the police's use of footwear impressions. The MPS's 'Treadware' system takes footwear impressions on a scanner that arrestees walk over as they enter a custody area and they are encouraging other forces to consider the system. DCI Julie Anderson of the MPS, who has helped develop the Treadware system, is in the process of evaluating its use. The national use of footwear impressions, other than on a casework basis, will depend not just on that (and probably other) evaluations but – because footwear impressions will be competing within an increasingly crowded forensic marketplace – its relative cost effectiveness. As long as the PoFA rules on the retention of footwear impressions are subject to such broad and differing interpretation, the police and the Home Office may have difficulty in justifying the current confused state of affairs. In light of this, the taking, utility, storage and governance of footwear impressions would appear to be in need of re-examining.

3.2 PROVIDING ASSURANCE ON POFA COMPLIANCE

51. A key role of the Commissioner is to provide assurance, initially to the Home Secretary and then to Parliament, on compliance with the PoFA regime by the police in their use and retention of biometrics. Other than the previous section of this chapter, the rest of this report is about compliance with PoFA regulation of the use and retention of fingerprints and DNA.

52. The three independent Forensic Service Providers (FSPs)[59] contracted by police forces to process DNA samples 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

[58] With only duplicates being deleted, even then only if a request is made by the relevant police force.

[59] LGC Ltd, Orchid Cellmark Ltd and Key Forensic Services Ltd. At present the future of Key Forensic Services is in doubt since it is in administration.

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. Going forward 'PoFA compliance checks' will be formalised in the context of the current UKAS assessments conducted during visits by UKAS every other year. Once such assessments are fully working this will add to assurance about compliance. However, having discussed this with UKAS, I concluded that there is still a role for me to regularly visit the FSPs, at least for so long as they remain such a central part of the routine processing of DNA and its analysis. A number of comments and observations later in this report show the value of doing so.

53. As far as individual police forces are concerned, assurance around compliance given in previous Annual Reports was based on a number of inspection visits, some limited data collection and experience of the caseworking functions of the Commissioner. This year we have completed the process of initial visits to all police forces, or consortiums of forces, which began in 2014. Through these visits to forces I and my predecessor have identified a range of compliance issues, which were reported in previous Annual Reports. The fact of our visit certainly had the immediate effect of focusing forces on whether their procedures in relation to PoFA were adequate and compliant. In some cases our visit resulted in recommendations as to changes that would improve compliance and future visits will check how far these recommendations have been implemented; indeed, they provide a risk assessment basis for the future timetabling of visits. However, it has taken four years to complete the visits to all forces because the Home Office has rarely managed to staff my Office with its full staffing complement (4). At the time of writing I only have one member of staff but if full staffing can be maintained in future I intend to increase the number of visits to forces each year.

54. Even with an increased programme of visits in future it will still not be possible to visit all forces each year. As explained in last year's report, I intend to make more use of the range of data that is collected by the Home Office, police forces and others about biometrics and their use. This will become easier as new management information systems are put in place for DNA and fingerprints.[60] I have been working with FINDS within the Home Office to develop a data collection matrix with a view to implementing new reporting structures from April 2018.[61] Descriptive analysis of such data will provide an annual national picture of compliance, as well as how and to what extent this varies by force or biometric type and use.

[60] However, this will not be available for fingerprints until sometime next year.

[61] I am grateful to Kirsty Faulkner, Head of the Forensic Information Databases Service and Caroline Goryll and Andrew Thompson of FINDS-DNA for their help in this regard.

55. Under the forthcoming General Data Protection Regulations (GDPR) and Data Protection Act police forces will need to have, amongst other things, effective internal policies and an audit and compliance framework for their force procedures. I shall examine such systems to decide how well they are delivering PoFA compliance.

3.3 ASSURANCE IN NORTHERN IRELAND

56. The only assurance role that I fulfil in Northern Ireland is in relation to counter-terrorism holdings and the granting of National Security Determinations, since in this regard I have UK-wide responsibility. Parliament granted Northern Ireland an extension to the PoFA counter-terrorism transitional arrangement to allow for political agreement on legacy investigations to be reached. This extension comes to an end on 31st October 2018 and unless Parliament agrees to a further extension the police in Northern Ireland will have to either have awarded NSDs or destroyed legacy biometric holdings by that date (for further explanation see also Chapter 5 of this Report).

57. As regards the retention and use of biometrics under PACE (for non CT crime investigations) that is a devolved matter for the Northern Ireland Executive. The Executive has passed the legislation to implement PoFA equivalent provision under PACE and for the appointment of a Northern Ireland Commissioner for the Retention of Biometric Material, however it has not yet been possible to secure cross party support to introduce an Order to make provision for prescribed circumstances. This means that Northern Ireland has not responded to the judgment of the ECtHR in *S & Marper v UK*;[62] however, since this is a devolved matter, it is an issue for the Northern Ireland Executive.

3.4 PACE POFA COMPLIANCE: ISSUES IDENTIFIED IN PREVIOUS ANNUAL REPORTS

58. I reported last year that the police were largely compliant with the PACE requirements of PoFA, whilst drawing attention to a number of areas that needed clarification by way of further guidance. Some new compliance issues have emerged during the course of 2017 and these are discussed elsewhere, of which the use of the CPIA exemption[63] is giving me particular concern. Other than that I have seen nothing this year that casts doubt on my overall judgement as regards PACE compliance and it is clear that, generally, the police have worked hard to ensure that their processes follow the requirements of the legislation.

[62] (2008) 48 ECHR 1169

[63] PoFA introduced the rule that DNA samples taken under PACE must, as a general rule, be destroyed once a profile has been derived and certainly with 6 months. However, other legislation allows the police to keep DNA samples until a criminal investigation and allied disclosure arrangements are concluded. This is an exception under the Criminal Procedure and Investigations Act 1996 (known as the CPIA exception). See also paragraph 230 below.

59. Notwithstanding this overall assessment, those tasked with implementing PoFA have faced a series of challenges, some of which were matters of legal interpretation and others of technical implementation. Many of these issues were resolved during the initial implementation of the legislation but others are awaiting the Home Office to issue guidance as was reported in the last three Annual Reports.[64] In the Government's response to my 2016 Annual Report Baroness Williams of Trafford recognised this, stating:

> *"You note that progress has been made in agreeing guidance to forces on matters of legal interpretation and technical implementation...You recommend that guidance must be issued more quickly in future. I agree that guidance should be issued more quickly than in the past and expect this to be done now responsibilities have been agreed".*

Nevertheless, it is the case that guidance on some matters is still awaited, even though some of these issues have been awaiting resolution for over four years.

LEGAL COMPLIANCE ISSUES

60. One issue of legal compliance that has been clarified and resolved during 2017 is that guidance has been issued, by FINDS-SB on 28 February 2017, on the treatment of matches against biometric material held unlawfully on the national DNA and fingerprint databases.[65] This refers to a situation where biometric material which should have been deleted matches against a previously unidentified crime scene finger mark or DNA profile on the national databases. If the evidence of such a match by this software was used in a prosecution then it could be challenged as inadmissible since the biometrics were held unlawfully at the point at which the match occurred.

61. The new guidance essentially makes three recommendations. Firstly, police forces should always carry out thorough checks as to whether a match has been made to lawfully retained biometric material. Secondly, police forces should seek to update all relevant records on the Police National Computer (PNC) and therefore trigger the deletion of biometric material as quickly as possible following the conclusion of an investigation so as to minimise the risk of unlawful matches. Thirdly, if a match is deemed to be unlawful it should not be disclosed or used evidentially unless a Chief Officer decides that the relevant offence is so serious as to justify releasing the information and ultimately putting the evidence of the match before

[64] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015,* at paragraphs 65-93, 214-259 and 262-275 and *Annual Report 2016*, at paragraphs 64 to 82.

[65] For a discussion of the need for such guidance see *Commissioner for the Retention and use of Biometric Material, Annual Report 2015* at paragraphs 263-267.

a court for a judge to decide if the public interest outweighs the fact of the unlawful retention. [66]

62. The issues that remain outstanding concern the drafting and updating of guidance to police forces on the meaning and correct application of PoFA. These were discussed at length in my last Annual Report and in my predecessor's last two Annual Reports but still remain to be dealt with. They are as follows in order of priority:

- Guidance on the use of 'Under Investigation' markers on the PNC following a match against the national DNA and fingerprint databases without a corresponding arrest;[67]
- Guidance on re-taking fingerprints and DNA samples from an arrested person;[68]
- Guidance on the application of the CPIA exception in respect of DNA samples;[69] and
- Matters arising as a consequence of wrongful arrests and mistaken identity.[70]

63. It is not clear to me when this outstanding guidance will be issued. This means that even if guidance is issued during next year it will be almost five years since PoFA was implemented. A way must be found so that if further guidance is needed it can be drafted and issued at greater pace.

GOVERNANCE STRUCTURES AND A NEW LEGAL ISSUE

64. I have previously reported on the fact that until recently the police national fingerprint databases, which are held on IDENT1, did not have a comparative governance structure to that in place for the National DNA Database.

65. The National DNA Database Strategy Board, now known as the Forensic Information Databases Strategy Board (FINDS-SB)[71] was put on a statutory footing under the provisions of the Protection of Freedoms Act 2012 and the governance rules now form part of the Police and Criminal Evidence Act 1984 at section 63AB(6). The current governance rules that formalise arrangements for the National DNA Database are in the process of being extended to cover the police national fingerprint databases. The basis for the inclusion of fingerprints will be the same as for DNA profiles in that the governance rules will apply to fingerprints

[66] This position may need to be re-examined when the new Data Protection legislation comes into force later this year since such unlawful matches could be regarded as a breach that has to be reported to the Information Commissioner.

[67] Ibid at paragraphs 271-272.

[68] Ibid at paragraphs 92-93 and 240-241.

[69] Ibid at paragraphs 181-188, 191 and 209-210.

[70] Ibid at paragraphs 257-259.

[71] The FINDS Strategy Board was previously briefly named the National DNA Database and Fingerprint Databases Strategy Board and was referred to as such in my 2016 Annual Report.

taken under both PACE and the Terrorism Acts. The powers accorded by these Acts are permissive and invested in Chief Constables who are data controllers in respect of the information loaded to those databases. The chair of FINDS-SB acts as data controller in common. The revised governance rules were tabled for agreement at the March meeting of FINDS-SB and attained National Police Chiefs' Council approval in November 2017. They are currently awaiting ministerial and Parliamentary approval.

66. As part of the process of aligning the governance structures for both DNA and fingerprints, the chair of FINDS-SB has sought to map the organisations which have access to the IDENT1 data platform, and the legal basis and the purpose for them doing so. Under the revised governance rules, all organisations that have access to IDENT1 will come under the governance of FINDS-SB and will be required to demonstrate a legal basis for access, conform to information assurance requirements and be subject to a privacy impact assessment. Myself and the Information Commissioner, and the Forensic Science Regulator, are observers at the FINDS-SB and will report on compliance with the aforementioned to the extent that such access falls within our respective areas of oversight.

67. PoFA, whilst setting down the rules within which law enforcement bodies must operate for the taking, storing, searching and deletion of DNA samples, profiles and fingerprints is silent as regards the operation of the databases and most importantly who should have access to them.

68. Within the national fingerprint database (IDENT1) there are a number of separate police collections of fingerprints. For example, there is the Police National Fingerprint Database (PNFDB) but also a separate Police Counter Terrorism Database. When IDENT1 was created it was purely used for police fingerprint databases. However, when the military started collecting fingerprints during their operations that meant that they needed a fingerprint database. The Ministry of Defence (MoD) was therefore given permission in 2010 to have their own, separate, cache of fingerprints within IDENT1. This cache is the only non-police collection within IDENT1. Hosting the MoD cache within IDENT1 was deemed a cost-effective solution since the IDENT1 system was already operational and commercially proven.

69. The difficulty around access to the records held on police databases has come to the fore as the MoD wish to check whether fingerprints taken or found during military operations abroad match to persons known to the UK police or immigration authorities or match crime scene fingerprints held by the police. In order to perform these checks a search must be made against the Police National Fingerprint Database (PNFDB).

70. It seems to me to be in the public interest that such searches should be possible, to support military operations abroad and counter-terrorism operations at home. However, such inter-departmental searching of biometric records should have a lawful basis and agreed governance arrangements.

71. The Protection of Freedoms Act (PoFA) put in place a set of rules for the retention and use of DNA and fingerprints by the police and other law enforcement agencies which are specified in the legislation. The MoD police and the other military police are listed as law enforcement agencies who can ask for searches against the PNFDB through the powers laid down in the PACE (Armed Forces) Act 2006.[72]

72. It would appear that the MoD are not currently searching via the routes permitted by the aforementioned powers but instead the searching is being carried out by the Defence Scientific & Technology Laboratories (Dstl) which is the research and technology arm of the MoD. They say they are doing so on the basis that they are not searching for law enforcement purposes but rather for purposes of national security.

73. The Chair of the FINDS-SB became aware that Dstl (on behalf of the MoD) have been searching beyond the MoD's own cache into the PNFDB on IDENT1. He and I have been discussing this matter with the MoD to understand why they are searching and on what legal basis.

74. It is not disputed that the MoD are entitled to search within their own cache within IDENT1 outside of the governance put in place by FINDS-SB under PoFA. The issue is the legal basis for Dstl searching the rest of IDENT1.

75. The National Police Chiefs' Council (NPCC) represents all Chief Constables, who are the data controllers of all of the police fingerprint collections on IDENT1. There therefore remains a question as to whether the NPCC accept the current position and continued Dstl searching across IDENT1 or whether they wish to ask further questions about the legal basis of and governance of such searching.

76. I can fully appreciate that the police need to be aware if a subject known to them for other reasons has been identified as either connected to an act of terrorism abroad or is present in theatre during a military operation. I can also understand that the military need to know if someone in theatre during an operation is known to the police in the UK (for example for force protection purposes). For these reasons I am not challenging the utility of such information sharing because I believe them to be in the public interest. Nevertheless, the mechanism for such searches should be transparent, lawful and be subject to clear governance. In passing PoFA, Parliament put in place a clear legal framework for the police use of fingerprints and its governance. That raises the question of whether a non-law enforcement agency should have the ability to search a police national biometric database unfettered by the requirements laid on the police and governance to which the police are subject.

77. This immediate issue, however, has wider implications when considered against the background of the Home Office Biometric Programme (HOB) which is developing and will

[72] As amended by PoFA.

soon start to deliver a new generation of data platforms, initially to replace existing databases. However, these new platforms are different in that they are designed to be multi-user on which logically separated databases can sit. That means that in future there will be a biometric data platform on which different agencies may hold their biometric database. Indeed, the new fingerprint data platform will hold both the police national fingerprint databases and the immigration fingerprint database. Since the biometric holdings of different agencies of government may have different legal or governance frameworks regulating both the use of biometrics and whether they are open to any other agency, then there will need to be clear access rules and a macro governance framework for those data platforms to ensure that only those who have lawful, approved access to specific databases are able access to them.[73] If this is not properly thought out and implemented as the new data platforms go live, then the situation which has allowed Dstl access to the PNFDB without clear governance arrangements in place, could emerge in other areas. It also raises the question of whether there ought to be oversight of that framework in addition to that provided by the Information Commissioner as is the case for the police use of biometrics.

78. Furthermore, the aforementioned also raises questions as to the mechanisms, and oversight, if any, of the transfer and retention of biometrics for national security purposes by different government agencies[74].

TECHNICAL ISSUES REQUIRING LEGISLATIVE CHANGE

CONVICTIONS OUTSIDE ENGLAND AND WALES

79. The 2015 Annual Report detailed the retention regime for individuals convicted of offences outside of England and Wales.[75] Biometric material taken from an arrestee could not lawfully be retained indefinitely simply because the individual in question had been convicted of the equivalent to a qualifying offence outside of England and Wales. If the police wished to retain the biometric records of such individuals and had no other basis for doing so, they had no option but to go back to those individuals and to take further samples and fingerprints from them.[76] This rule applied to those convicted of offences in Northern Ireland and Scotland.[77]

[73] This will remain the case unless Parliament enacts generic biometric use legislation and the open sharing of biometric data across government agencies.

[74] See also discussion on material held under section 18 CTA 2008 in Chapter 5 of this Report.

[75] Ibid at paragraphs 68-83. See also Appendix B of this Report.

[76] Ibid at paragraph 70.

[77] Ibid at paragraph 73.

80. Changes to the regime governing retention of biometrics on the basis of convictions outside of England and Wales was included in the Policing and Crime Act 2017, which received Royal Assent on 31 January 2017. The changes mean that all biometric material taken after 03 April 2017 from individuals in connection with an arrest in England and Wales, but who have previously been convicted of a recordable offence outside of England and Wales, may be held indefinitely on the national fingerprint and DNA databases without the requirement to take further samples/fingerprints expressly for that purpose. Although the relevant provisions[78] were commenced on 03 April 2017[79] the necessary changes to the PNC and the issuing of guidance to forces have not yet happened[80].

QUALIFYING OFFENCES

81. The 2015 Annual Report observed that there were a number of serious and equivalent offences that had seemingly been omitted from the list of qualifying offences as set out in section 65A PACE.[81] Furthermore, some law enforcement agencies also wanted the list to be extended: for example the National Crime Agency (NCA) wanted to see serious fraud added since they are often investigating serious international fraud and biometrics can be important in such cases.

82. Expanding the list of qualifying offences requires an appropriate Statutory Instrument to be approved by Parliament. It was planned that such an Instrument would be laid before Parliament in mid-2016, however this was further delayed due to ongoing discussions with the devolved governments in order to agree a definitive list of offences. I reported last year that the relevant secondary legislation was planned for 2017 but this has not happened. Home Office officials have now indicated that Parliamentary time is limited but they hope to be allocated time in 2018 to present the proposed changes, although at the time of writing this was still subject to confirmation. I further understand that a proposal will soon be circulated to policing and policy colleagues for comments on the proposed changes, although it is as yet still unclear what those recommended changes will be or when those changes, if agreed, will be implemented.

[78] See sections 70 and 71 of the Crime and Policing Act 2017 at

http://www.legislation.gov.uk/ukpga/2017/3/contents/enacted

[79] See *The Policing and Crime Act 2017 (Commencement No 1 and Transitional Provisions) Regulations 2017* at https://www.legislation.gov.uk/uksi/2017/399/regulation/6/made

[80] I understand that the changes to PNC are due to be implemented in May 2018 but that these will not be fully effective unless the equivalent qualifying offences in Scotland, Northern Ireland, Guernsey, Jersey and Isle of Man have been identified by the Home Office prior to that date.

[81] See *Commissioner for Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 65-67.

PROTRACTED INVESTIGATIONS AND THE RELEASE OF ARRESTEES OTHERWISE THAN ON BAIL

83. The 2015 Annual Report referred to problems in connection with protracted investigations and police practice of releasing arrestees otherwise than on bail when investigations into those individuals remain active.[82] This was leading to the unintended automatic deletion of biometrics. I indicated in my 2016 report that legislative changes to be introduced in early 2017 were expected to alleviate this issue. As anticipated the relevant sections of the Policing and Crime Act 2017 were commenced on 03 April 2017 with necessary changes to the PNC made and guidance issued in time for the commencement of the legislation.

84. The Policing and Crime Act 2017 has introduced changes to police force custody systems and the Police National Computer (PNC) which has enabled the police to release arrestees otherwise than on bail whilst an investigation continues without the risk of losing lawfully held biometric material. It should be noted that the new provisions apply only to those first arrested for an offence on or after 3rd April 2017. For those arrested on or before 2nd April 2017, the former rules will continue to apply. As such there is still a risk, albeit much reduced, that biometric material could continue to be lost erroneously until those legacy investigations are concluded.

85. Although the issues relating to the erroneous deletion of biometric material from the national databases in relation to the release of individuals otherwise than on police bail have been largely mitigated by the provisions within the Policing and Crime Act 2017, the changes to the legislation on pre-charge bail have raised other concerns in relation to the retention of biometric material from arrested persons. The new rules, as well as allowing for the release of suspects without bail, also introduce much more stringent requirements in respect of individuals released on pre-charge bail, including strict and much reduced timescales and fast-tracked escalation points for authorisation of bail beyond 28 days. There is a risk that investigations involving suspects who are released on police bail could therefore be prioritised by officers seeking to meet stringent bail targets whereas those investigations where the suspects have been 'released under investigation', without bail, may not be such a priority for investigators, leading to differential retention of biometric material.

86. At the time the changes were implemented I wrote to police forces to request that all forces keep records in relation to the number of persons 'Released Under Investigation' so that I can report on the situation. Moreover, in my visits to forces and in a note issued to police forces by my Office I have urged that, in the absence of pre-charge bail, the investigation should continue to be monitored and reviewed at regular intervals and should be conducted

[82] Ibid at paragraphs 56, 240-243 and 245(iii).

and concluded in a prompt and efficient manner. Every effort should be taken to ensure that once an investigation is concluded, the PNC is updated with the outcome of the investigation at the earliest opportunity to ensure that biometrics are not held for longer than is necessary.

87. It has recently come to my attention that some police forces are not monitoring cases where a subject has been released under investigation or updating the PNC at the end of the investigation in a timely manner in such cases. As a result there is now a strong likelihood of unlawful matches occurring with biometric records held in cases where a subject was released under investigation and the investigation has now ended, but the associated records have not been updated. I intend to write again to forces to reiterate the importance of regular monitoring and updating in such cases and I intend to keep this matter under review over the coming year. It is clear, however, that further changes need to be made to the PNC to ensure that forces are provided with an automatic reminder and are compelled to provide regular updates where a subject is released under investigation, as they were under the old bail rules.

VOLUNTARY ATTENDANCE

88. One other, probably unintended, consequence of the new bail regime has been an increase in the use of voluntary attendance. Before a lawful arrest can be made under section 24 of PACE, a constable must have reasonable grounds for believing that the arrest is necessary for at least one of the reasons detailed in section 24(5).[83] PACE Code G[84] requires that an officer should always consider if the necessary objectives can be met by other, less obtrusive, means. Where an arrest is not deemed necessary, people of interest to an investigation may be interviewed out of custody. Voluntary attendance is covered under section 29 of PACE 1984 and refers to the process whereby a person voluntarily attends a police station to assist the police with the investigation of an offence and that person is not under arrest.

89. As a result of visits to forces it has become apparent that the use of voluntary attendance, in lieu of arrest, is being used by all police forces to varying degrees and some forces have reported an increase in the use of voluntary attendance in response to challenging bail targets and other operational pressures.[85] As with many areas of policing, however, policies

[83] See also in this regard PACE Code G at Sections 2.4 to 2.7 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117583/pace-code-g-2012.pdf

[84] (at paragraph 1.3)

[85] Some forces have reduced their number of custody suites to save costs, sometimes resulting in long journeys to remaining custody suites for arrestees. The use of voluntary attendance is a way of avoiding these new costs but with the unfortunate consequence that biometrics cannot be loaded onto the national databases via PNC (because a PNC record, against which biometric records are recorded, can only properly be created following an arrest or summons) and there is no immediate available search of the national databases.

on voluntary attendance have been left to the discretion of individual forces to implement, thereby leading to an inconsistent approach nationally.

90. There is no standard process or clear guidance as to when or for what offences the voluntary attendance process is appropriate. Many police forces are also unclear as to when it is appropriate to obtain biometric samples from voluntary attendees. I have, further, seen examples where serious offences have inappropriately followed the voluntary attendance process, instead of that individual being arrested, with associated biometric samples taken under PACE.

91. In respect of biometric retention, risks have been identified where such inconsistencies have led to the following:

- Questions over whether biometric samples have been taken lawfully and what they can subsequently be used for.
- Missed opportunities to speculatively search individuals – some of whom are accused of very serious and/or sexual offences – against unsolved crimes due to DNA samples/fingerprints not being taken and loaded to the databases (IDENT1 and NDNAD) either because the individual has not been arrested, allowing their biometrics to be loaded to the national databases via PNC, or because biometrics have not been taken later where there has been a positive disposal or conviction.
- Missed opportunities where samples are taken inappropriately or not processed in a timely manner in accordance with PoFA deadlines for retention and destruction.
- Records of the voluntary attendance being incorrectly recorded on PNC as 'under investigation' where there has been no relevant arrest or disposal.

92. In response to concerns raised by my Office at FINDS-SB and elsewhere an expert network was convened in June 2017 to discuss the relevant issues and to formulate recommendations for national guidelines.

93. From the meeting it was clear that the inconsistencies across England and Wales posed potential risks to policing and a number of recommendations were formulated with a view to mitigating those risks. Those recommendations were approved and forwarded to the NPCC lead on custody and the NPCC lead on Fingerprints as well as the NPCC lead for forensics and the Chair of FINDS-SB. The recommendations included the need for:

a. a consistent national approach with a determined set of core criteria agreed at a national level to ensure as far as possible that the process is used in a fair and consistent manner by all police forces;

Further, without the facilities available in a custody suite (such as Livescan fingerprint machines and specially trained officers) biometrics, when taken, can be of poor quality, such as ink set fingerprints and incorrectly taken/handled DNA samples.

b. clearly articulated risks and priorities for mitigation of those risks;

c. transparent governance with the requirement that each force having a policy with clear routes for accountability, monitoring, oversight and escalation of relevant issues;

d. baseline reporting and collation of management information;

e. clear guidelines for when it is and is not appropriate to use voluntary attendance;

f. guidelines for when it is and is not appropriate to take biometrics from voluntary attendees;

g. improved training and awareness; and

h. investment in mobile technologies to aid the collection of biometrics outside of custody suites.

94. I understand that a national police-led group has been set up to develop Approved Professional Practice (APP) through the NPCC and College of Policing and that the recommendations set out above have been provisionally accepted by that group.

ISSUES RELATED TO THE OPERATION OF PNC

DELAYS IN UPDATING THE PNC

95. My predecessor repeatedly raised concerns about delays and/or errors in updating the PNC with officials at the Home Office, with the FINDS-SB and with others and I have echoed those views.[86] 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. In response to my previous Annual Report Baroness Williams of Trafford stated on behalf of the Government that:

> *The National Police Chiefs' Council will shortly be issuing a letter to forces reminding them of the existing requirements around updating PNC. In September, they will issue new operational guidance for all forces setting out how PNC should be used".*

I have not had sight of such guidance and to date have not been able to ascertain if it was ever issued.

WANTED/MISSING AND LOCATE/INFO MARKERS

96. As reported in previous years,[87] and until recently, any wanted/missing or locate/info marker placed on a PNC record will prevent the deletion of biometric records even if those

[86] See Commissioner for the Retention and Use of Biometric Material Annual Report 2016, at paragraphs 77-79.

[87] Ibid at paragraphs 221-222 and 227-228 respectively.

records cannot lawfully be retained. In December 2016 it appeared that the biometric records of approximately 8,690 individuals were being wrongly retained, as a result of this problem.

97. Although I understand that it is unlikely that this problem can be wholly resolved, implemented changes to the categorisation of Wanted/Missing and Locate/Info markers on the PNC, known as 'Operational Information', should mean that the number of unlawfully retained biometric records is substantially reduced (2016 estimates suggest a reduction of approximately 80%). I have not been able to obtain the relevant figure for 2017 and will therefore continue to pursue this matter.

BIOMETRICS COMMISSIONER 'UZ' MARKERS

98. 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 Criminal Records Office (ACRO) with a monthly report which gives brief details of every UZ marker that appears on the PNC.[88] This enables me to monitor the number of UZ markers in use and to check the data provided against my own records.

99. As of 20 December 2017, a total of 352 UZ markers were in use by forces in England and Wales. That figure breaks down as follows:

TABLE 12: Biometrics Commissioner 'UZ' Markers by Force (20 December 2017)

Force	No. UZ Applied[89]
MPS	117
South Wales	79
City of London	36
West Yorkshire	27
Bedfordshire	20
Thames Valley	10

[88] Special thanks to Jessica Mullins of ACRO Criminal Records Office for her assistance in collating and reporting the relevant data.

[89] It should be noted that the number of UZ markers in use includes cases where a decision is yet to be made by the relevant force whether to make an application to the Biometrics Commissioner under section 63G PACE and therefore the number of UZ markers in use will inevitably be higher than the number of applications received under that section.

Kent	10
Northumbria	9
Hertfordshire	6
Devon & Cornwall	6
Durham	5
West Mercia	5
Cambridgeshire	5
Humberside	3
North Yorkshire	2
Cleveland	2
Warwickshire	2
North Wales	2
Cheshire	1
South Yorkshire	1
Derbyshire	1
Essex	1
Gloucestershire	1
Gwent	1

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

- There have been numerous instances of the inappropriate use of a UZ marker, for example where a UZ marker has simply been erroneously applied or applied and then no formal application for retention under section 63G PACE has been made.
- 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 the biometrics can be retained only for three years from the date they were taken.[90]

101. 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 above and have largely been resolved by the changes to the bail process set out in the Policing and Crime Act 2017. I shall continue to monitor the ongoing issues with regards to the proper and timely administration of the PNC and the management of Wanted/Missing and UZ markers placed on the PNC. Consequently I continue to urge the Home Office and others involved with the administration of PNC to alert forces to the risks identified as regards biometric retention and to provide them with practical guidance on the steps that can and should be taken to minimise those problems.

102. An underlying problem is that PNC is now a very old system and therefore difficult to re-programme as changes take place. The PNC is due to be replaced as part of the Home Office's National Law Enforcement Data Programme (NLEDS) but not until 2020.[91]

[90] 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.

[91] The National Law Enforcement Data Programme is working to replace PNC with the new Law Enforcement Data Service in line with the PNC contract end date of December 2020.

4. APPLICATIONS TO THE COMMISSIONER TO RETAIN BIOMETRICS

4.1 APPLICATIONS TO THE BIOMETRICS COMMISSIONER TO RETAIN BIOMETRICS

103. Chief Officers of Police in England and Wales can apply to the Biometrics Commissioner to retain the biometrics (DNA profile and/or fingerprints) of people, with no prior convictions, who have been arrested for a 'qualifying offence'[92] but neither charged nor convicted.[93] In order for the police application to be approved they must persuade the Commissioner that retaining the biometrics will be useful in the detection, prevention or deterrence of crime.[94]

104. The person who is the subject of such an application must be notified by the police that an application has been made and must be told upon what grounds the application is being made. The subject of the application has the right to make their own representations to the Commissioner challenging the application for retention of their biometrics.[95]

105. If the Commissioner accepts such a police application then the fingerprints and/or DNA profile may be kept for three years from the date when the DNA sample and/or fingerprints were taken.[96] At the end of that period the police may apply to a District Judge for a further retention period of two years. The relevant statutory provisions are set out in full at **Appendix B**.

APPLICATIONS

106. From when the relevant sections of PoFA came into force on 31 October 2013 to 31 December 2017, 493 such applications to the Commissioner were received. Of those 493 applications:

- 91 were made in the period 31 October 2013 to 31 August 2014;
- 118 were made in the period 01 September 2014 to 31 August 2015;
- 177 were made in the period 01 September 2015 to 31 December 2016; and

[92] Generally more serious violent, sexual offences, terrorist offences, burglary and robbery. See: The Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013.

[93] Under section 63G of PACE as inserted by PoFA.

[94] Under section 63G(4) of PACE.

[95] See section 63G(5) and (6) of PACE and further http://www.gov.uk/government/publications/principles-for-assessing-applications-for-biometric-retention. 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.

[96] (See footnote 78 in last year's Report)

- 107 were made in the period 01 January 2017 to 31 December 2017.[97]

107. Over that latter period, the average rate of applications has remained broadly consistent with that in 2013/14 and in 2017 at between 9 and 10 per month, even though the number of forces making such applications has increased.

108. The great bulk of the 209 applications submitted up to 31 August 2015 were made by the Metropolitan Police Service (MPS) and during that period only 8 of the other 42 forces in England and Wales made applications. Since September 2015 a far larger number of forces have submitted applications and I reported a year ago that 23 of the forces in England and Wales had made one or more applications. That figure has now risen to 27. 15 forces have yet to make an application – See further Table 13.[98] During 2017 the MPS made 50 of the 107 applications to the Commissioner, with the other 57 made by 16 different forces.

TABLE 13: Number of Applications to the Commissioner by Force (Year ending 31 December 2017)

Force	Applications
Metropolitan Police	50
Yorkshire & Humberside[99]	13
Thames Valley	11
Kent	9
Devon & Cornwall	5
Northumbria	4
Cambridgeshire	4
South Wales	3
Bedfordshire	3
Warwickshire	2
Hertfordshire	1
West Mercia	1
Cleveland	1
TOTAL	**107**

[97] The different time periods given are reflective of the reporting periods of each of the previous Annual Reports (see also footnote 2, Chapter 1).

[98] Avon and Somerset, Norfolk, Gloucestershire, Essex, Derbyshire, Cumbria, North Wales, Dorset, City of London, Durham and Greater Manchester have also made applications since 31 October 2013 but not in the current reporting period.

[99] Collaboration on biometric retention consisting of West Yorkshire, South Yorkshire, North Yorkshire and Humberside.

109. In the 50 months since the introduction of the PoFA Regime on 31 October 2013 (i.e. to 31 December 2017), applications to the Commissioner were received and determined as follows.

TABLE 14: Applications to the Commissioner to Retain Biometrics for Qualifying Offences under section 63G PACE.

	31 October 2013 to 31 December 2017	01 January 2017 to 31 December 2017
Total Applications	**493**	**107**
- Representations from subjects	62 (12.6%)	9
Concluded by end 2017[100]	**439 (89.0%)**	**89**
- Approved wholly or in part	287 (65.4%)	62
- Refused	100 (22.8%)	19
- Withdrawn	52[101] (11.8%)	8[102]

STATUTORY BASIS FOR APPLICATIONS TO THE COMMISSIONER

110. Applications to the Commissioner may be made either in respect of the special characteristics of the victim (section 63G(2) PACE) or the general prevention and detection of crime (section 63G(3) PACE).

111. Between 31 October 2013 and 31 December 2017, 283 applications were made in relation to victim characteristics and 210 were made for the more general purpose of the prevention

[100] Cases concluded during 2017 do not correlate exactly with cases received in 2017 as there is necessarily a time lag between receiving and concluding a case.

[101] Includes 3 applications that were rejected as invalid.

[102] Includes 1 application rejected as invalid.

or detection of crime.[103] In a number of the former, more than one of the 'victim criteria' were satisfied.

Table 15: Statutory Basis for Applications to the Commissioner

	Applications received	Approved wholly or in part	Refused
Victim Criteria[104]	**283**	**148**	**77**
- Under 18	239	132	64
- 'Vulnerable'	19	6	6
- Associated with subject of application	25	10	7
Prevention/detection of crime	**210**	**139**	**23**

4.2 PRELIMINARY APPLICATIONS, INTERIM NOTIFICATIONS AND ONGOING COMPLEX INVESTIGATIONS

PRELIMINARY APPLICATIONS

112. In anticipation that forces might have concerns about the extent to which they would be required to disclose confidential information to a subject of an application, my predecessor put in place a procedure for so-called 'Preliminary Applications'. By that procedure it is open to a Chief Officer to raise any such disclosure concerns with my Office before they submit a formal application or send a notification letter to the subject of the application.

113. In fact matters of disclosure have arisen only relatively rarely and to 31 December 2017 only 9 such applications have been made. All bar one of these preliminary applications have gone on to become full applications.

INTERIM NOTIFICATIONS

114. A significant number of cases referred to my Office since the commencement of PoFA have involved individuals 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

[103] In a not insignificant number of 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.

[104] In some cases more than one of the victim criteria are satisfied. Figures in the table relate only to the primary victim criterion given.

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

115. In such circumstances, rather than making an application under section 63G as soon as it was decided that the qualifying offence should be NFA'd – the police should write to the subject informing him or her that such an application might be made in the future when the ongoing prosecution is concluded. This is known as an 'Interim Notification' and it does not require any action by the subject at that point. 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'.[105]

116. 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 December 2017 my Office was informed of 129 Interim Notifications. As at that latter date, 25 of those Notifications had been followed by applications under section 63G and 98 had 'lapsed' either because (in 79 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 19 cases) it was decided not to proceed to a full application.

ONGOING COMPLEX INVESTIGATIONS

117. My predecessor's 2015 Report[106] 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;
- he 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
- he 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.

That case has now been concluded.

118. My Office is aware of a number of investigations of this sort and receives regular monthly updates on the cases concerned. The issues in respect of biometric retention in complex and protracted investigations should be mitigated by the changes to the legislation

[105] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2014* at paragraphs 61-66. 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.

[106] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraph 56.

governing police bail contained in the Policing and Crime Act 2017. The legislation is not retrospective so a small number of cases where there is still an ongoing protracted investigation that predates the legislation are still affected.

4.3 APPLICATIONS TO A DISTRICT JUDGE (MAGISTRATES' COURT)

119. Whilst I can consent to the retention of biometrics for those arrested for, but not charged with, a qualifying offence, that retention period will only be for a maximum of three years from the date the biometrics were taken. The retention period for those charged with, but not convicted of, a qualifying offence is similarly three years. If the police wish to retain the relevant biometrics for a further period of two years in either circumstance they can apply to a District Judge.[107]

120. My last Annual Report recorded that by 31st December 2016 only 6 applications to a District Judge had been made. Since then no further applications have been made. Given that so few applications have been made it is difficult to predict to what extent such applications will be made in the future.

4.4 ISSUES ARISING FROM RETENTION APPLICATIONS TO THE COMMISSIONER

121. The applications received since the commencement of the relevant sections of PoFA have raised a number of questions which are discussed below. These were discussed in detail in my last Annual Report and are addressed more briefly this year.

WHY ARE NOT ALL POLICE FORCES MAKING APPLICATIONS?

122. The legislation does not require the police to make such applications to the Commissioner but rather allows them to do so. Each force, therefore, must decide whether to devote resources to making such applications or to other tasks. In other words, they have to make a cost-benefit judgement and forces have differed in their conclusions.

123. It should be noted that whilst the present rate of applications enables me, in the usual course of events[108], to respond to applications made under section 63G within a reasonable period, this might not be possible if the application rate were to significantly increase.

HOW ARE APPLICATIONS MADE AND PROCESSED?

124. Police make applications to the Commissioner on a standard template designed to provide evidence in relation to the key factors and principles the Commissioner must consider. In addition, the police must attach the detailed case file to evidence the case for retention that

[107] See Section 63F of PACE as inserted by section 3 of PoFA.

[108] It should be noted that my Office was understaffed for the entirety of last year and particularly so in the last quarter, resulting in a significant backlog of cases at year end.

they have put forward in the application. The application must be authorised by a Chief Officer of Police and is usually submitted to my Office electronically.

125. In every instance, the subject of an application is told if that application has been refused or approved. Where an application is approved, detailed reasons are only provided as a matter of course to subjects who have made representations to me.[109] The submission of representations is taken as both confirmation of the subject's contact details/preferred mode of contact and as an indication that the subject would want to see full reasons for the decision.

126. In all other cases, a shorter decision letter is sent informing the subject that a decision has been made to approve the application and summarising the consequences of that decision. The subject may ask for the detailed reasons for the decision within 28 days of the decision date.

127. All correspondence is sent by Royal Mail First Class Recorded Delivery unless the subject requests otherwise. Where a subject is untraceable or is known to have left their last known address a decision letter is not despatched but is instead 'served to file'.

ON WHAT GROUNDS DOES THE COMMISSIONER DECIDE APPLICATIONS?

128. In order to make an application the police have to demonstrate that, whilst the subject was not charged for the offence at issue, there is evidence to show that it is likely that the subject of the application was involved in the act, that retaining the biometrics for 3 years will either be a deterrent to future criminal action or aid in the prevention or detection of future crime, and finally that the interference in the subject's privacy is proportionate given the public benefit that is likely to result. I must weigh the evidence on each of these factors, in each case, before reaching a decision. The Commissioner's core principles and approach to assessing these relevant factors is set out in a document issued by my Office entitled *'Principles for Assessing Applications for Biometric Retention'*.[110] Furthermore, and as was contemplated by section 24 of PoFA, formal guidance about such applications was published by the National DNA Database Strategy Board.[111]

129. Since the subject of an application will not have been charged, the police or the CPS will have concluded that either:

[109] Since the conclusion of the application process can happen some time after the last police contact with the subject, this process has been adopted to avoid the dispatch of sensitive personal information unless and until the Office has a confirmed current address for the subject.

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

[111] https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace

- the available evidence is unlikely to support a successful prosecution;[112] or
- charging the subject would not be in the public interest.[113]

130. If the former, the subject of an application may regard it as strange that where there is insufficient evidence to justify charging them with the offence there can be sufficient grounds to justify retention of their biometrics. In fact the so-called 'charging threshold' requires that the evidence is such for there to be a realistic prospect of conviction and that depends on judging how far the evidence is likely to stand up to cross examination. However, I am not bound to consider the evidence against the subject to the higher criminal standard, instead I will require that the criteria as set out in the 'Principles' document are satisfied and that retention of the subject's biometrics is considered 'appropriate'. It is noteworthy that although the number of representations to me by the subjects of applications is small, in those I have received the subject often objects to an application on the grounds that the police have investigated their actions but it has been decided not to proceed with a prosecution.

131. If the subject was not charged because it was judged not to be in the public interest to do so, or because the complainant refused to support a prosecution, that test is independent of the strength of the evidence against that individual.

132. If I am so persuaded, I then have to be satisfied that retaining the biometrics at issue will reduce the risk or deter further offending or will help in the detection of future crime. For example, in relation to some crimes biometrics are *often* of importance in identifying the offender (e.g. burglary), for others they *may* be (e.g. rape) and others *rarely* (e.g. domestic violence). It is for the police to persuade me that in the particular circumstances, as set out in the application, retaining the subject's biometrics will be useful.

---

[112] See http://www.cps.gov.uk/victims_witnesses/reporting_a_crime/decision_to_charge.html. The prosecutor must first decide whether or not there is enough evidence against the defendant for a realistic prospect of conviction. This means that the magistrates or jury are more likely than not to convict the defendant of the charge. If there is not a realistic prospect of conviction, the case should not go ahead, no matter how important or serious it may be.

[113] See http://www.cps.gov.uk/victims_witnesses/reporting_a_crime/decision_to_charge.html. If the crown prosecutor decides that there is a realistic prospect of conviction they must then consider whether it is in the public interest to prosecute the defendant. While the public interest will vary from case to case, broadly speaking the more serious an alleged offence the more likely it will be that a prosecution is needed in the public interest. A prosecution is less likely to be needed if, for example, a court would be likely to fix a minimal or token penalty, or the loss or harm connected with the offence was minor, and the result of a single incident. The interests of the victim are an important factor when considering the public interest. Crown Prosecutors will always take into account the consequences for the victim and any views expressed by the victim or the victim's family.

133. Even if both these conditions are fulfilled, I must judge whether retaining the biometrics would be proportionate in the particular case by balancing the public benefit from retention against the interference in individual freedom that it will involve. Where the subject is under the age of 18 I must additionally bear in mind the principle established in S and Marper v United Kingdom[114] that *'particular attention should be paid to the protection of juveniles from any detriment that may result from the retention … of their private data'*,

134. Failure to meet any of these conditions will lead me to refuse an application.

WHAT TYPES OF OFFENCES LEAD TO APPLICATIONS?

135. Only 'qualifying offences' can be the basis of an application but, as can be seen in Table 16, the majority (61%) of applications are for sexual offences.

TABLE 16: Outcome of Applications to the Commissioner to Retain Biometrics for Qualifying Offences under section 63G PACE (31 October 2013 – 31 December 2017)

Offence Group	Total Applications	Approved	Refused	Withdrawn	Yet to be Decided
Murder, Attempts and Threats to Kill	11	5 (45.5%)	4 (36.4%)	0 (0%)	2 (18.2%)
Sexual Crimes	303	158 (52.1%)	80 (26.4%)	30 (10%)	35 (11.6%)
Assaults	82	56 (68.3%)	9 (11%)	12 (15%)	5 (6.1%)
Robbery	53	40 (75.5%)	1 (2%)	8 (15.1%)	4 (7.5%)
Burglary	30	18 (60%)	5 (16.7%)	0 (0%)	7 (23.3%)
Other	14	11 (78.6%)	0 (0%)	2 (14.3%)	1 (7.1%)
Total	**493**	**287**	**100**	**52**	**54**

[114] (2008) 48 EHRR 1169 at paragraph 124

136. The high percentage of sexual offences seen to date is indicative of both the evidential difficulties involved in these types of cases and the fact that the handling by the police and criminal justice system of allegations of sexual crimes has been controversial for some time. Often there are no witnesses to these types of offences and many cases involve the uncorroborated word of one party against the other. A decision not to pursue a charge or prosecution against the accused may consequently result in applications for biometric retention being made to the Commissioner.

137. A particular feature of the applications received by my Office in the last year has been the increase in applications related to sexual contact between young people. The CPS has extensive guidelines in respect of charging for sexual offences. One is to the effect that the charging decision for sexual offences should be the same as for other offences but with a more proactive approach to evidence building.[115] Conversely, the guidelines also advise that it may not be in the public interest to criminalise sexual behaviour, especially between young people[116], and therefore balancing these guidelines can be difficult. For example, sexual penetration between a 15 year old male and a 12 year old female is rape, even if both parties say they freely consented, and so such an offence should be charged. On the other hand, the offence involves sexual behaviour between young people and a decision may be taken that prosecution of those involved would not be in the public interest. If the latter decision is made the police may, and often do, choose to apply to retain the biometrics of those arrested.

138. Furthermore, some alleged sexual offences take place in a familial context or involve sexual experimentation by children where action other than prosecution, such as a multi-agency intervention, might be felt to be more appropriate. In such scenarios, it remains open to the police to apply to retain the biometrics of those accused.

139. Not all such applications will be approved. The most common reason for refusal is where the alleged sexual offence has taken place between family members or familiars and there is no reason to suggest that the subject may turn their attention to strangers. In such cases the identity of the alleged offender is not in doubt and the utility of retaining biometrics is diminished.

140. It is evident from the applications received by my Office that there is a general belief amongst the police that minor sexual offending, or familial sexual offending, will lead to sexual offending of increasing gravity or stranger attacks. There is some evidence to

[115] See: http://www.cps.gov.uk/legal/p_to_r/rape_and_sexual_offences/cps_policy_statement/

[116] http://www.cps.gov.uk/news/fact_sheets/sexual_offences. However, children of the same or similar age are highly unlikely to be prosecuted for engaging in sexual activity, where the activity is mutually agreed and there is no abuse or exploitation.

support this belief but it is by no means conclusive[117] and in any case the evidence refers to overall statistics and does not provide a basis for predicting the future behaviour of an individual.

141. The issues discussed above are part of a more general problem: when determining applications, the Commissioner is being asked to agree to the retention of biometrics on the grounds that offending and possibly more serious offending is likely, whether for sexual or other crimes, even though – in the eyes of the law – the subject of that application is innocent of any alleged offence. Unfortunately, there is no systematic knowledge base against which such claims can be made or judged. This is a gap that the College of Policing could seek to fill. Absent such a knowledge base the police make applications and I must make the best decision I can on the basis of the facts in each individual case.

142. Since the first applications to the Commissioner under section 63G to be approved were in relation to material taken in November 2013, it now seems pertinent to examine the rate of conviction for subjects during the 3-year period that their biometrics are retained. To this end I have kindly been provided with some data by Chief Constable Simon Bailey of Norfolk Police which relates to further police contact with a subject following an application made under section 63G (in relation to the first 407 applications made to the Commissioner). The police contact records includes further arrests, charges, convictions and other disposals by the police. [118] It is still too early to draw any conclusions, given the limited length of time that has passed and the size and limitations of the data set. Nevertheless, it is possible to make the following observations:

    i. Around one third of the individuals who have been the subject of a section 63G application since 31 October 2013 (to 28 February 2017) have come to further police attention (i.e. were at least arrested again) since the arrest that was the subject of the application.[119]

---

[117] See e.g. Soothill, K et al: *Murder and Serious Sexual Assault: What Criminal Histories Can Reveal About Future Serious Offending*, Home Office: Police Research Series, Paper 144, 2002

[118] At this early stage of analysis a differentiation has not been made between applications approved and refused. The length of time since the first arrest also varies as the data relates to applications made from 31 October 2013 to 28 February 2017. For obvious reasons a greater proportion of the subjects of earlier applications have come into further contact with the police.

[119] For juveniles taken separately this figure is around one quarter. These re-arrest rates are very similar to the *re-offending* rates for *convicted* offenders (30% in general and 42% for juveniles) see; //www.gov.uk/government/uploads/system/uploads/attachment_data/file/676431/proven-reoffending-bulletin-jan16-mar16.pdf. However, this is not the comparison that is really required to judge the utility of section 63G since that would compare subsequent offending rates of those arrested but neither charged nor convicted in general with the sub-group of that same population subject to a section 63G application and whether agreed to or not. However, subsequent conviction rates for those arrested but neither charged nor convicted are not routinely available.

ii. The 137 individuals who came to police attention again, did so in relation to 667 further alleged offences, indicating a significant level of possible re-offending within this group.

iii. Of these 667 further alleged offences, 213 have now resulted in a conviction (including cautions, court convictions and penalty notices), 41 are still outstanding and 413 resulted in no conviction (including 324 NFAs). It is notable that in relation to around half of arrests the contact ended with no further action being taken.

iv. Of those 137 individuals who came to police attention again after a section 63G application, 78 individuals now have a conviction (including cautions, court convictions and penalty notices), which is 19% of all subjects of section 63G applications and lower than the re-convicted rate for those convicted (see footnote 119).

v. There appears to be little, if any, correlation between the type of offence in relation to which the section 63G application was made and the type of offence(s) in relation to which the subject has subsequently come into further contact with the police[120]. This is contrary to the aforementioned (in paragraph 140 above) argument, often advanced by the police, that minor sexual offending will lead to further, more serious sexual offending.

143. The argument after the S and Marper judgment as to whether the evidence existed that the biometrics of those arrested but neither charged nor convicted should be retained, as laid out in the then Labour government's discussion paper: *Keeping the Right People on the DNA Database: Science and Public Protection (2009,)*[121] was heavily criticised at the time and the utility of the subsequent section 63G of PACE (as amended by PoFA) is still unknown. Moreover, whilst the preliminary findings above begin to give us insight into possible re-offending behaviour of section 63G subjects, the data currently available does not assist in identifying whether and to what extent retained DNA or fingerprints were a factor in any of the further arrests or convictions.

WHY DO SO FEW SUBJECTS OF APPLICATIONS MAKE REPRESENTATIONS?

144. Parliament was careful in legislating to allow the subject of an application to the Biometrics Commissioner to challenge that application by making representations but to date only a minority of the subjects have done so – see Table 17.

[120] For example, of 75 juveniles subject to an application in relation to a sexual offence 20 came to further contact with the police. Of those 20 only 6 were in relation to a further sexual offence. Other contact was in relation to a wide range of offences including violent, drug and driving offences.

[121] See: http://webarchive.nationalarchives.gov.uk/20100408151339/http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-consultation2835.pdf?view=Binary

Table 17: Representations by Subjects and Outcomes (year ending 31 December 2017)

Applications	Totals	Representations made by subject of application
Approved Applications	287	32 (11.1%)
Refused Applications	100	21 (21%)

145. As explained above, when making an application to the Biometrics Commissioner to retain biometric material, the police must provide the subject of that application with sufficient details of their application and the reasons for it to allow that individual to make reasoned representations. Most forces do this by providing the subject with a copy of the application which they have submitted to my Office. In a small number of cases I have formed the view that, because of the limited disclosure 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 such cases, my Office has informed the relevant force that their notification was inadequate and I have only taken into account those factors of which the subject has been made aware. On other occasions my Office has alerted applying forces to significant omissions from their Notification Letters and, where appropriate, a revised Notification Letter has been issued.

146. Issues of disclosure are difficult to balance because the police may occasionally have good reason not to inform a subject of information they hold, for example where this would identify and potentially put in danger an informant. Conversely, however, it is difficult to see how a subject's right under PoFA to challenge an application can be preserved if such an application depends on evidence that the subject is not able to see. Where issues concerning disclosure are identified at an early stage, forces are encouraged to make use of the Preliminary Application Process.[122]

147. Notwithstanding issues of disclosure, I do not believe that the few examples of inadequate notification are the reason for the low number of representations received by my Office. It is acknowledged that some subjects may not receive notification of an application if their contact details change, but it appears that most do receive the notification and so lack of knowledge of an application and the grounds for it does not appear to be the main reason for the low number of representations received from subjects.

148. It is conceivable that subjects of applications may not be highly literate and/or may find the task of challenging the case advanced by the police daunting[123]. More worrying is if subjects

[122] See Section 4.2 of this Report above.

[123] In general the offender population has relatively high levels of poor literacy and education compared to the general population as well as higher rates of mental illness and drug taking: see, e.g.:

believe that they will not be listened to or that they simply wish, following an NFA for an alleged offence, to bring to an end what has been a lengthy and stressful experience.

149. The information given to subjects about their right to make representations is accurate but not easy for the subject of an application to understand. I think that the information ought to be re-examined to see if it could be made more intelligible to an arrestee population or even whether an alternative to a written format might be better? The Home Office's Biometrics and Forensics Ethics Group have also raised concerns about the intelligibility of written information provided to arrestees. The Ethics Group have therefore been doing some work on the use of plain English in such circumstances.

150. The low rate for the submission of representations is a problem in that it suggests that the protection for subjects of an application intended by Parliament is not working as expected.

4.5 THE TREATMENT OF CHILDREN AND YOUNG PEOPLE

151. One aspect of the section 63G application process to which the previous Commissioner drew attention is the general policy adopted by the Commissioner's Office and the police to address correspondence only to the subject of an application unless and until they expressly authorise us to do otherwise. Where, however, there is a reason to suspect that a subject is a minor or vulnerable, letters are normally headed 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*."

152. This policy was adopted on the basis that such applications usually include information of a sensitive nature and young people 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.

153. This situation was, however, unsatisfactory and led to concerns within the Commissioner's Office that, due to data protection concerns, children were being denied the support of their parents or guardians to make effective representations to the Commissioner. In practice it is unrealistic to think that most young people – and certainly children – would be able to fully understand the process in which they find themselves and to make well-reasoned representations to the Commissioner without support.

154. The obvious answer to this problem would be to ensure that the parent or guardian is made aware when an application is made to the Commissioner to retain the biometrics of a child or young person, unless there are strong reasons not to do so, and that the child or young person understands their rights to make representations.

---

http://www.prisonerseducation.org.uk/media-press/new-government-data-on-english-and-maths-skills-of-prisoners and publications.parliament.uk/pa/cm201213/cmselect/cmhaff/184/18409.htm

155. In December 2016, I discussed the problem with Chief Constable Olivia Pinkney, the NPCC lead on the policing of children and young people. She agreed that the current practice is not satisfactory and has undertaken to work towards a revised procedure that can be discussed by the NPCC.

156. The intention is that up-to-date contact details of the parent or guardian will be checked by the police when they make an application to the Commissioner under section 63G of PACE. Unless the subject objects, or the circumstances of the young person indicate that it would be appropriate to do otherwise, the parent or guardian will be informed of the application and the right to make representations and the outcome of those applications will be communicated to all parties. Unfortunately this matter has not been progressed since my last Annual Report and the situation regarding writing to minors therefore remains unsatisfactory.

4.6 EXTENDING THE QUALIFYING OFFENCES LIST

157. Applications to retain the biometrics of those who have been arrested but neither charged nor convicted can only be made in respect of 'qualifying offences'. There is an intention by the Home Office to review the list of qualifying offences. Depending on the extent to which that list is extended, the proposed changes could lead to a significant increase in the number of applications to retain the biometrics of those who have neither been charged nor convicted of an offence and so have the potential to change the overall proportionality balance within PoFA. Any such changes could also increase the Commissioner's case load. As such I have asked that a risk assessment be conducted in this regard in order to determine the possible resource ramifications of any proposed change.

4.7 MINISTRY OF DEFENCE USE OF SECTION 63G APPLICATIONS

158. Section 113 sets out which areas of PACE apply to the armed forces subject to any modifications that the Secretary of State considers appropriate.[124] The Act is supplemented by the Police and Criminal Evidence Act 1984 (Armed Forces) Order 2009. The PACE (Armed Forces) Order 2009 concerning Service Police has been amended to mirror PACE as amended by PoFA.[125] This gives broadly equivalent, but not identical provisions, on the retention and use of biometric material by the Service Police.

159. The Service Police have concurrent jurisdiction (with civilian police) and I understand that most Service Police arrests within the UK are taken and processed by Hampshire Police on their behalf. Service Police would only have sole jurisdiction when overseas dealing with uniformed officers or their families and civil servants.

---

[124] See Schedule 16 paragraph 105(2) of the Armed Forces Act 2006.

[125] See Police and Criminal Evidence Act 1984 (Armed Forces) (Amendment) Order 2013 at http://www.legislation.gov.uk/uksi/2013/2554/made

160. Sections 20 (Appointment and functions of Commissioner) and 21 (Reports by Commissioner) of PoFA do not amend PACE, meaning that these powers are specific to the PoFA legislation and are not applicable to the Armed Forces. As such, I do not have direct independent oversight of the retention of biometric material taken specifically by the Service Police under the PACE (Armed Forces) Act, although the PACE military holdings on the national databases are subject to the same automated retention rules[126] as are in place for civilian arrestees and appropriate rules regarding quality and accreditation equally apply. I do, however, have oversight of the use of biometric material taken by civilian police forces held on the national biometric databases and I consider that to include any searches being made against national civilian holdings by Service Police.

161. The retention regime introduced by PoFA in respect of national security material taken under terrorism legislation[127] is somewhat different. In such cases the Royal Military Police, individual Service Police Forces and the Ministry of Defence Police are specifically listed as forces for these purposes and therefore any material retained or used by them is subject to the amendments introduced by PoFA and, moreover, my oversight.

162. During the reporting period, my Office has received queries from military police in respect of potential applications to retain the DNA profile and fingerprints of individuals arrested for, but not charged with, qualifying offences[128] and qualifying service offences. In response to those queries I have advised that there appears to be no equivalent provision in Section 15 of the PACE (Armed Forces) Order 2009 to that in Section 63G PACE (as inserted by Section 3 of PoFA) where civilian police forces in England and Wales may make an application to the Commissioner to retain biometric material for a maximum of three years (or five years on further application to a District Judge). This appears, on the face of it, to be an inconsistent approach in the law in terms of how those arrested by the civilian and service police forces are treated when arrested for alleged offences of an equivalent nature.

163. For the Service Police to be able to apply for retention of biometrics for those arrested but not charged of serious offences, the Ministry of Defence would require a mechanism to amend PoFA and to extend the function of the Biometrics Commissioner.

[126] See section 15 of PACE 1984 (Armed Forces) Act 2009 (as amended by Police and Criminal Evidence Act 1984 (Armed Forces) (Amendment) Order 2013).

[127] See section 63U and further Parts I and III of Schedule 1 to PoFA 2012.

[128] Under section 65A PACE.

5. BIOMETRICS AND NATIONAL SECURITY

5.1 POLICE BIOMETRICS AND NATIONAL SECURITY DETERMINATIONS

164. PoFA introduced stricter rules as regards the retention by police in England and Wales of biometric material which has been obtained from unconvicted individuals. PoFA also introduced stricter rules as regards the retention by police anywhere in the United Kingdom of biometric material which has been obtained from unconvicted individuals of national security interest and that cannot lawfully be retained on any other basis.

165. A responsible Chief Officer or Chief Constable[129] has the power under PoFA to order that such biometrics should be retained on grounds of national security. They may only do so by agreeing to a National Security Determination or 'NSD'. The power to make an NSD applies across the UK and is not limited to England and Wales because national security matters, unlike criminal matters, are not devolved.

166. An NSD must be in writing and lasts for a maximum of 2 years beginning with the date it is made.[130] An NSD may be renewed for a further period of 2 years and can be considered for renewal on any number of further occasions. For further details of these provisions see **Appendix C**.

5.2 COMPLIANCE WITH POFA

167. I have reported elsewhere in this Report that as far as compliance with those elements of the Police and Criminal Evidence Act 1984 as modified by PoFA is concerned the police are generally compliant and all police forces, despite specific areas of concern, are making considerable efforts to be compliant. I reported the same thing last year and my predecessor did similarly the year before that.

168. As in previous years, the situation as regards compliance with the counter-terrorism provisions of PoFA is less favourable. The problems that I and my predecessor have identified both in this and previous years have largely been brought about by the counter-terrorism command (SO15) of the Metropolitan Police Service failing to bring their legacy holdings of biometric material into compliance with the requirements of PoFA.

169. Last year I reported that I had been assured that the difficulties around legacy compliance had all been dealt with. I therefore regret to report that during the course of 2017 a further significant legacy PoFA compliance issue has emerged, as detailed below.

---

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

[130] The statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different (see further Appendix C).

5.3 COUNTER-TERRORISM DATABASES

GENERALLY

170. Biometrics retained under an NSD are held on separate counter-terrorism DNA and fingerprint databases.[131] All new DNA profiles and tenprint fingerprint sets which are loaded to the NDNAD and IDENT1 are checked against those CT databases.[132]

171. At the commencement of the 'biometric' provisions of PoFA on 31 October 2013, the DNA profiles and/or fingerprints of some 6,500 identified individuals were being held by police forces on the national CT databases. The comparable figure as at 31 October 2015 was some 7,800 and as at 31 December 2017 was some 11,841. Those latter figures encompass both new additions to the databases since 31 October 2013 and deletions from those databases after that date.

172. Of the individuals whose biometric records were being held by the police on those databases as at 31 December 2017 some 2,358 (i.e. about 20%) had never been convicted of a recordable offence.

[131] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraph 167, for further details.

[132] For further information about the cross-searching of those databases, see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2014* at paragraphs 170-174.

TABLE 18: Holdings of biometric material on the CT Databases (year ending 31 December 2017)[133]

		2016	2017
DNA	**DNA**	**608**	**9,072[134]**
	- Of which unconvicted	65 (11%)	2,171[135] (24%)
Fingerprints	**Fingerprints**	**8,478**	**9,966**
	- Of which unconvicted	1,185 (14%)	1,623 (16%)
TOTALS	**Total Holdings**	**9,086**	**19,038[136]**
	- Of which unconvicted	1,250 (14%)	3,794[137] (20%)
	- *New material*	*695* *(56%)*	*2,632[138]* *(69%)*
	- *Legacy material*	*555* *(44%)*	*1,162[139]* *(31%)*

(Source: SOFS)

[133] For 2014 and 2015– see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2014 and 2015* at section 3.

[134] Includes 7,197 individuals whose fingerprints are also held on the CT databases. Figure given for DNA in 2016 was given in error only for 'DNA only' holdings hence the apparent large increase.

[135] Includes 1,436 individuals whose fingerprints are also held on the CT databases. Figure given for DNA in 2016 was of 'DNA only' holdings.

[136] This is the total number of individual biometrics on the CT databases. It includes the 7,197 individuals whose DNA and fingerprints are on the CT databases. Taking this into account there is material relating to 11,841 individuals on the CT databases

[137] Relates to 2,358 individuals. Figures for last year related to individuals rather than material.

[138] 1,394 DNA profiles and 1,238 sets of fingerprints.

[139] 777 DNA profiles and 385 sets of fingerprints.

GOVERNANCE

173. My predecessor reported that the CT databases suffer a 'governance deficit' as regards the comprehensive governance arrangements and protocols that might be reasonably expected.[140] Since taking up post I have reiterated the need for proper governance arrangements and have indicated that I expect appropriate arrangements and documentation on the CT database and PoFA compliance in general to be put in place. The FINDS-SB intend to add the CT databases to their governance where it will be dealt with in the same way as other police DNA and fingerprint database holdings. This is a significant step in improving the governance of the CT databases and essential as the new HOB databases come into use.

174. That leaves the question of the governance of the process for retaining CT biometrics operated by the counter-terrorism command (SO15) of the Metropolitan police. Last year I reported that I had sought re-assurance on this from the Commander of SO15 because of previous failures to deal properly with legacy holdings.[141] I was informed that 'in future the PoFA CT Programme Board will report to a National Security Biometrics Board, chaired by the Commander of SO15. This is a higher level of accountability than applied in the past and will apply performance management indicators to monitor performance.' I welcomed these proposals last year and they have been implemented during the year but the extent to which this has been successful is discussed below.

5.4 THE NSD PROCESS

175. As explained above, deciding whether an NSD should be approved is a matter for Chief Officers of police.[142]

176. Counter-terrorism policing in the UK consists of regional Counter-Terrorism Units (CTUs) based in the English and Welsh regions and Scotland, coordinated by SO15, and in Northern Ireland by the Police Service of Northern Ireland (PSNI).

177. Initially applications to Chief Officers for NSDs are put together either by SO15 or PSNI. PSNI deals with all Northern Ireland cases but SO15 oversees all other cases and most of those are signed off by the S015 Commander. Applications for biometrics taken by regional CTUs are signed off by their respective Chief Officers.

---

[140] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraph 170.

[141] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016 section 5.8.*

[142] 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.

178. The information on which NSD applications are made is largely drawn from police records of previous criminal justice system contacts and police intelligence. Often additional information will come from the Security Service, who will provide their holding code[143] as additional supporting data for the NSD decision.

179. If it is decided that an NSD application should be made, the supporting data is summarised on the application form. A case is also presented as to whether retaining biometrics is necessary on grounds of national security and, if so, whether such retention would be proportionate. SO15/PSNI add a reasoned recommendation to the application which also proposes to the Chief Officer whether the supporting intelligence/evidence is adequate to justify making an NSD. There is Statutory Guidance on what should be considered, further discussion of which can be found in **Appendix C**.[144]

180. 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.

181. If an application for an NSD is approved, the decision of the Chief Officer is recorded at the end of the application together with his or her reasons for approving the application. That document then becomes the NSD and is available to me for my review. My Office also receives copies of any applications that are refused by Chief Officers so that I can oversee the entirety of the process.

182. 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. Professor Clive Walker of the University of Leeds has written to me challenging this position and cited a number ECtHR judgments[145] that would support making the fact of biometric retention known to the subject. My initial response to him was to point out that since NSDs often depend on intelligence then giving the reasons for an NSD might compromise future intelligence or its source. He quite reasonably has pointed out to me that whilst this might be true in some cases this does not speak to simply making the fact of biometric retention known, nor to all cases. PoFA itself is silent on the

---

[143] For a discussion of the Security Service holding codes see: Attacks in London and Manchester, March-June 2017, Independent Assessment of MI5 and Police Internal Reviews, December 2017, 1.5.

[144] See also *Protection of Freedoms Act 2012: Guidance on the making and renewing of National Security Determinations allowing the retention of biometric data.* (http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf)

[145] He cites: 'In the jurisprudence of the ECtHR, an active notification requirement will be relevant to the compliance with Articles 8 and 13 of the ECHR. See inter alia Klass v Germany, App no 5029/71 A28 (1978); Weber and Saravia v Germany, Application No 54934/00, 29 June 2006; Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria, Application No 62540/00, 28 June 2007; Kennedy v United Kingdom, Application No 26839/05, 18 May 2010; Uzun v Germany, Application No 35623/05, 2 September 2010.'

issue but the introduction of the EU's new General Data Protection Regulations (GDPR) and the new Data Protection Bill into UK law may also raise the question of whether notification of biometric retention should be given. I am grateful to Professor Walker for raising this issue with me and I agree that there is a general principle that where a power is being used that may be to the detriment of an individual that person ought to know on what grounds that power is exercised and have the opportunity to challenge it. In this case I see the issue as to whether there is a countervailing public interest, in the case of counter-terrorism, in restricting the application of the general principle as a matter, in the first instance, for Parliament and then the courts. PoFA implies that there is a case for restriction but does not set out the reason for this[146].

ROLE OF THE RESPONSIBLE CHIEF OFFICER

183. An NSD may only be made or renewed by a responsible Chief Officer or their nominated deputy of the force in which the biometric material was taken.[147]

184. When making an NSD, the Chief Officer must be persuaded that retention of the biometric material at issue is necessary on grounds of national security and that retention is proportionate, balancing the public interest against the subject's right to privacy.

185. I have been generally impressed with the care taken to identify the cases for which an NSD might be properly made or, conversely, rejected. Recently, however, I have had concerns that Chief Officer decision making was becoming more varied as experienced Chief Officers were being replaced by less experienced new Chief Officers. I had particular concerns where NSDs were agreed to with little police evidence but a Security Service holding code and/or where Chief Officers had not given clear reasons for their decision. I challenged a number of these cases and I wrote to all Chief Constables asking them to remind all Chief Officers deciding NSD cases of the guidelines[148] and that they must give reasons for their decisions.

186. I can report that since then the decision making has improved although I still have some concerns about unevenness across the NSD decision making process. It has been suggested to me that this process could be made less uneven if fewer Chief Officers were involved in the process; for example that one Chief Officer were to decide NSDs for each CTU. At present this is not possible because PoFA requires a Chief Officer from the force that took the biometrics to decide whether to make an NSD. The Government may wish to consider amending this as a result of the review of CT legislation ordered by the Prime Minister.

---

[146] I am also grateful to Professor Walker for allowing me to quote his views in this Report.

[147] That deputy must be of at least the rank of Assistant Chief Constable or Commander in the Metropolitan Police Service.

[148] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf

187. My oversight of the NSD process and the data in this Report, shows that by no means all potential cases are considered for an NSD and not all of those put forward for an NSD are accepted by Chief Officers. Notwithstanding my comments above it is my view, based on my observations of the process and of the NSDs both made and declined by Chief Officers, that in the vast majority of cases, proper judgement is being exercised.

188. Overall, I can confirm that the NSD process operates so as to fulfil the conditions for the granting of NSDs as laid down in PoFA and the accompanying statutory guidance.[149]

THE ROLE OF THE COMMISSIONER

189. Once a Chief Officer has decided to make an NSD, the NSD IT system automatically informs my Office. My job as regards NSDs is laid down in PoFA and is to keep under review:

    (i) every NSD made or renewed; and

    (ii) the uses to which material retained pursuant to an NSD is being put.

    If I do not think that retention of the relevant material is necessary or proportionate I have the power to order its destruction.[150] This is a significant power which, given the threats being managed, I should exercise carefully.

190. It should be noted that my duty to keep national security biometric retention under review only applies to the police holdings of such material and does not to apply to holdings by non-law enforcement agencies, such as the security and intelligence services or the military. Law enforcement bodies for these purposes are defined in PoFA[151] and have access to the various police biometrics databases.

COMMISSIONER'S REVIEW OF NSDs MADE OR RENEWED

191. My primary role in relation to national security matters is to keep under review every NSD made or renewed. In doing so I should not be re-examining the case afresh, since I would be repeating a decision-making process already followed by a Chief Officer of police. Rather, my role is to examine each application to ensure that the evidence exists on which a 'reasonable Chief Officer' could have made an NSD.

192. Where I do not judge this to be the case I will identify my concerns and challenge the police as to whether they have any further information that could justify making an NSD. Given the importance of getting NSD decisions correct, I have felt it right to continue my

[149] See further *Protection of Freedoms Act 2012: Guidance on the making and renewing of National Security Determinations allowing the retention of biometric data.* (http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf)

[150] PoFA sections 20 (2)(a & b),(4) and (5).

[151] See Parts I to VII of Schedule 1 of PoFA.

predecessor's policy of awaiting the result of any challenge before exercising my power to order the destruction of the relevant material at issue.

193. As can be seen in Table 19, 322 NSDs were made by SO15 and PSNI during 2017. I supported 310 of the NSDs made in 2017 and I raised challenges in 34 of the cases I examined. In 12 of these I ordered the destruction of the biometric material since I was not persuaded by the police response to my challenge, to the extent that I could not assess the NSD made as being necessary and proportionate.

194. Most of the challenges I have made have been because either I had doubts as to whether the case presented offered a current Security Service holding code, or where there was an apparent conflict in the information provided. I have been particularly concerned about the first of these doubts: namely that the threat assessment used as part of the justification for an NSD is up-to-date and based on current information. I have discussed these concerns both with the police and the Security Service and they have agreed that where I have such concerns and challenge an NSD they will ensure that all information is updated.

195. In most cases the police are either able to give me further information from their own sources or given to them by the Security Service who have provided updated supporting data to support their case for retention. Sometimes this further material strengthens the case for an NSD, but sometimes the opposite, and I have ordered the deletion of the biometrics.

THE USE TO WHICH NSD MATERIAL IS PUT

196. I am required to keep under review the process of making NSDs and the use to which retained material is subsequently put. I have seen nothing to suggest that material is being used otherwise than for permitted purposes. However, the continuing legacy workload (see Section 5.8 below) as well as lack of staff in my Office has limited the time that could be spent on this second requirement.

197. I have been provided with some data by Secure Operations – Forensic Services (SOFS) which begins to provide a picture of the use to which retained material is being put. Over the past 12 months there have been 36 print to print hits against subjects with NSDs upon loading fingerprints to the Police National Fingerprint Database. There has also been one fingerprint to mark hit against a subject with an NSD[152]. There have been 10 matches against a subject with an NSD upon loading a subject DNA profile to the NDNAD and there have also been

[152] This represents only partial data in terms of fingerprint matches as SOFS were unable to provide data on subsequent matches against the national database at the time of reporting. Efforts are being made to improve IT/reporting systems to ensure full reporting in future.

two crime stain sample matches to a subject with an NSD[153]. Subsequent searches against the NDNAD found 25 subjects about whom an NSD had been made. A further 14 subjects who did not have an NSD at the time of the NDNAD search/match are now subject to an NSD.

198. All of the matches against material held in relation to an NSD are viewed by SO15. Fingerprint to mark and crime stain to subject profile matches assist the police in investigating crime in the usual way. Except that, were it not for the NSD, the fingerprints/DNA profile in question would not have been retained. However, it is evident that the numbers of these types of match are small. Print to print or subject to subject matches may assist SO15 in building up an intelligence picture about the individual to whom the match relates.

199. I am informed by PSNI that to date there have been no biometric matches against material held under the NSD process. This is based on searches of the material against both local and national fingerprint and DNA databases. It must be noted however that NSDs made by PSNI represent only a small proportion of the total number of NSDs, for example only 36 of the 325 NSDs I supported this year were made by PSNI (29 of which were renewals). The reasons for this are outlined in paragraph 5.7 below.

200. I intend to make reviewing the use to which NSD material is being put one of my priorities in the coming year and I have asked SOFS to keep more detailed records of the use of retained material.

5.5 NEW MATERIAL

201. 'New Material' refers to biometrics taken after PoFA came into effect on 31 October 2013. For these biometrics the retention period which applies in the absence of an NSD 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 are summarised at **Appendix C**.

5.6 CASES REVIEWED AND NSDs MADE

202. By 31 December 2017 the cases of approximately 5,800 individuals who had never been convicted of a recordable offence but whose biometric records were nonetheless being

[153] There were also 15 subject matches in relation to subjects who now have an NSD made in relation to them but did not at the time of the load.

retained on the national CT databases had been reviewed by SO15/PSNI for NSD purposes.[154]

TABLE 19: NSD decisions year ending 31st December 2017[155]

	2016	2017
Total possible NSDs applications processed	**713**	**1170**
- Renewal NSDs considered	-	158
- New NSDs considered	-	1012
- NSDs approved by Chief Officer	591	322
○ *Renewals*	-	77
○ *New NSDs*	-	245
- NSDs declined by Chief Officer	122	27
○ *Renewals*	-	3
○ *New NSDs*	-	26
- NSDs supported by Commissioner	543	325
- NSDs challenged or further information sought	96	34
- Destruction ordered by Commissioner	42	26

[154] Special thanks to staff within SO15, SOFS and PSNI for their help in compiling the relevant data and more generally for their assistance during the 2016/2017 reporting year.

[155] I reviewed a number of NSDs made by SO15 at the end of 2016 in 2017. 15 of the 325 NSDs I supported during 2017 were made in 2016 and 14 of the 26 NSDs where I ordered destruction of material during 2017 were made in 2016.

5.7 NSDs IN NORTHERN IRELAND

203. Currently the Police Service of Northern Ireland Legacy Investigations Branch and Police Ombudsman have responsibility to investigate deaths in Northern Ireland related to the historic conflict in Northern Ireland ('The Troubles'). It is anticipated that this role will shortly transfer to the 'Historical Investigations Unit'. In June 2016, a Statutory Instrument was laid before Parliament by the Northern Ireland Office amending the existing Transitional Order and thereby extending the Legacy period in Northern Ireland for a further two years, until 31 October 2018.[156] This Order applies only to Northern Irish biometric material taken under counter-terrorism powers and because Legacy records may be needed as part of that historical cases review process, it *"seeks to ensure that the timing of commencement of the destruction provisions in relation to biometric material taken under counter-terrorism powers in Northern Ireland allows for political agreement on legacy investigations to be reached"*.[157]

204. The upshot of this amendment is that generally national security Legacy cases in Northern Ireland will no longer be reviewed as to PoFA compliance until after 31 October 2018. However, unless a further such Statutory Instrument is passed by Parliament, then PSNI must either consider legacy material for an NSD or delete it by 31st October 2018.

205. A number of legacy cases were reviewed and a small number of NSDs made prior to the Parliamentary extension being granted. These NSDs, once made, are now subject to the PoFA bi-annual renewal requirement.

206. New biometrics taken in Northern Ireland as part of a national security investigation under the Terrorism Act 2000 (TACT) since the commencement of PoFA must be treated in the same manner as elsewhere in the UK and be fully PoFA compliant. PSNI are fully compliant in relation to material taken under counter-terrorism powers since the commencement of PoFA.

5.8 SECTION 18 COUNTER TERRORISM ACT 2008

207. The majority of biometric records held for national security purposes are taken following arrests or detentions within the UK under PACE or national security powers. Biometrics which are received from other agencies within the UK, such as UK Visas and Immigration (UKVI) or from foreign law enforcement agencies, which are not subject to existing UK statutory regulation, are subject to the provisions contained in section 18 of the Counter Terrorism Act 2008 (CTA).

[156] http://www.legislation.gov.uk/uksi/2016/682/contents/made

[157] http://www.publications.parliament.uk/pa/ld201617/ldselect/ldsecleg/25/2504.htm

208. Put shortly, section 18 CTA (as amended by Schedule 1, Part 3 of PoFA) states that all identifiable[158] biometric records (fingerprints and DNA profiles), which are not subject to other statutory regimes, may be retained for a maximum of 3 years, with a possibility to extend that retention period by way of a National Security Determination approved by a Chief Officer. That NSD must be made in writing and is valid for a maximum renewable period of 2 years. All material not subject to an NSD at the expiry of the initial 3 year retention period must be destroyed and cannot be used in evidence or otherwise after that date. However, under the same provision if the biometric records are not identifiable then they can be kept indefinitely.

209. I understand that the MPS wrongly assumed during the transition phase to implement PoFA that biometric data received from outside of the UK could be retained indefinitely. My Office raised with the MPS from 2014 onwards our view that unless the records were not identifiable then after three years they could no longer be lawfully held under section 18 and we urged them to seek legal advice**.**

210. The MPS sought legal advice in January 2017 as to the lawfulness of their holdings and came to the conclusion that large numbers of records held on the CT databases, and which it previously considered as not coming under the regime set out in section 18 CTA, are in fact affected by that retention regime and should have been considered during the transitional period between 31 October 2013 and 31 October 2016.

211. Following that decision and extensive discussions with me and officials in the Home Office, the MPS embarked on a thorough review of its holdings to determine the number of records affected. It has concluded that 978,248 records should have been considered under the legacy provisions but were not.

212. In September 2017, SO15 commenced an extensive risk assessment project, in collaboration with international partners and law enforcement agencies to determine the purpose and relative merits of retaining the various datasets which amounted to 978,248 records in total. This review was concluded by February 2018 and found that 191,827 records were not identifiable and so could be lawfully retained indefinitely under section 18. After a detailed and time consuming review of all the records SO15 concluded that the great majority of all of the holding could be deleted. Of the non identifiable records, 190,597 are therefore to be deleted and 1,230 retained. Of the remaining identifiable records already held for more than three years 173 are to retained and the others (i.e. the vast majority) are in the process

[158] i.e. all records which have demographic identifiers attached to them. Records which cannot and have never been identifiable by the agency holding the record (i.e. anonymised biometric records or unidentified crime scene profiles) are not subject to the 3 year retention rule until and unless they are identified/attributed to a known individual.

of being deleted[159]. Of the records deleted, some may still be available for searching by SO15, if they are retained on databases held by non-policing agencies, such as the MoD or UKVI.[160]

213. At present SO15 hold copy records of some asylum claimants and these similarly fall under the constraints of section 18. However, when it becomes possible for the process of searching for latent matches between the CT fingerprint database and the immigration and asylum database to be automated, SO15 will no longer need to keep these records on the CT database. That will happen on present plans by the end of April 2018. At that point SO15 intend to delete their current asylum holdings since it will no longer be necessary to retain them separately.

214. To avoid further issues of this sort in the future, from 01 October 2017, all data received by MPS's Forensic Services Secure Operations from UK partners for retention within the CT forensic databases for the purposes of national security shall not be in identifiable format. This will allow for indefinite retention on the CT Forensic databases until and unless that data matches against a known individual.

215. Presently SO15 is holding some section 18 material unlawfully and has been for some time. I have asked the MPS to report to me any instances of matches against unlawfully held material. To date I have not been informed of any such matches.

216. There now remains a question around the identifiable records older than three years that SO15 wish to keep in the interest of national security. SO15 propose to bring those records within section 18 as soon as possible by awarding the cases NSDs. However, they propose to do that by making three single NSDs to cover three separate bundles of records, totalling 173 records. I remain to be persuaded that such an approach would be lawful.

217. PoFA applies only to the police use of biometrics and police databases but we have now entered a world in which the police, and indeed other government agencies, are increasingly searching against each others' holdings. Any of these searches may be allowed by the legislation applying to each database but there is a lack of general legislation and governance for intra-government data searching. It is not clear whether anyone in government has detailed or overarching knowledge of this process, yet it is evolving rapidly. Furthermore, the HOB programme and probably other such programmes elsewhere in government are developing new multi-agency data platforms that will facilitate such cross-database searching. The fact that SO15 are deleting some records from their databases

[159] 46 records held for less than 3 years will now become part of the normal review process.

[160] The number of deleted records that are duplicated in this way is impossible to measure because the content of these databases is dynamic.

knowing that they may be able to search them in other agency's databases could either be regarded as circumventing the constraints of section 18 or simply recognising that those constraints do not reflect the present reality. The issue is not whether access to such data by SO15 is necessary for counter-terrorism purposes and therefore in the national interest (it almost certainly is) but whether the government's strategy for the use of biometrics and other data needs to address intra-government data sharing and what, if any, legal constraints and governance should be put in place.

5.9 OTHER MATTERS

FUTURE NSD WORK LOAD

218. PoFA provides that NSDs should run for a maximum of two years from the date they are agreed by a Chief Officer, but that they can be renewed on any number of subsequent occasions as long as it remains necessary and proportionate to hold the material. The limited retention period no doubt reflects Parliament's concerns that sensitive biometric holdings relating to individuals who have not been convicted of an offence or, in the case of Schedule 7 TACT detainees, even arrested[161] should be reviewed regularly and independently overseen.

219. NSDs are being reviewed at two yearly intervals as Parliament intended. For some NSD cases, my judgment is that the evidence/intelligence against the relevant individuals is such that they could be granted for longer than two years.

220. The Government may wish to consider this issue as part of the CT legislation review ordered by the Prime Minister.

DATA LOSSES

221. I and my predecessor have both reported, in previous annual reports, that a number of IT issues, procedural and handling errors have led to the loss of a significant number of new biometric records that could and should have been retained on the grounds of national security. During 2017, the new biometrics of 13 additional individuals have been lost. The biometrics of 6 of those 13 were lost because SOFS did not pass the case to SO15 before the relevant biometrics reached their statutory deletion date (or so close to that date that an NSD could not be made)[162]. The biometrics of the remaining 7 individuals were lost due to administrative errors, in particular in relation to how the cases were recorded on PNC.

[161] Individuals detained and questioned under Schedule 7 TACT need not be arrested in order to take biometrics.

[162] 3 of these losses were historical, having occurred in 2013 (2 cases) and 2015 (1 case) but the losses were only discovered and recorded during 2017.

222. I reported last year that I was satisfied that measures had been taken within SO15/SOFS to remedy the causes and mitigate the effects of these type of problems where appropriate. Whilst I understand that this work is still ongoing it is disappointing to report that losses of biometric data have continued, albeit that they are small in number, but the MPS are putting in place a new IT platform which they hope will deal with this problem in future.

PRE-EMPTIVE NSDS

223. I reported last year my significant concerns about the police applying for 'pre-emptive' NSDs.[163] If a person of national security concern is arrested for a criminal offence under PACE their biometrics may be kept under the normal crime related rules discussed earlier. If that arrestee is subsequently convicted of a recordable offence the individual's biometrics can be kept indefinitely and an NSD to retain the biometrics will be unnecessary. If, on the other hand, a decision is made to take no further action ('NFA') against an arrested individual who has no previous convictions, the biometric material will be deleted forthwith and there will be no time to consider a case for retention under an NSD. This has created a dilemma for the police, which to avoid they are applying for an NSD where a person of national security concern has been arrested but the result of the further investigation is still unknown.

224. There is nothing unlawful about making such applications but these pre-emptive NSD applications may well be unnecessary in some cases, either because the biometrics could in the event be retained under PACE retention rules or the investigation does not ultimately provide evidence to justify retention. For these reasons, I have made clear to the police that I do not think that such pre-emptive NSDs are proper except in cases where other justificatory evidence already exists. What is particularly difficult is that I have seen pre-emptive NSDs where the evidence did not, in my judgement, reach the thresholds for an NSD even though after further investigation it may have done so and if, after challenge this does not change then deletion has to be ordered.

225. The most straightforward solution to this problem would be for the police to be allowed a short grace period after an NFA decision, where the individual is of national security interest, to allow for an NSD application to be considered. In non-national security cases the police have 28 days after an NFA decision to make an application to me to retain the biometrics in relation to qualifying offences and a similar period for NSD applications would avoid the need for pre-emptive NSD applications.

226. I understand that the Home Office's Office for Security and Counter-Terrorism (OSCT) could change their guidelines to make such a period of time available and they have agreed to consider doing so at the earliest opportunity. SO15 have objected that they will need more than the 28 days allowed in non CT cases and this is now for OSCT to decide.

[163] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016 paras 207-213.*

227. A related issue regarding individuals arrested otherwise than under section 41 TACT is that there is often a delay in notifying SO15 that an individual of national security concern has been NFA'd. Unlike the situation with the national biometric databases, CT biometric material is not automatically weeded from the CT databases when it reaches its statutory expiry date. SO15 rely on the accuracy of PNC to determine whether biometric material is lawfully held when the NSD application is prepared. Any delay in updating the PNC with the outcome of an investigation or any delay in notifying SO15 that an investigation has come to an end may lead to applications for NSDs inadvertently being made in respect of material which is no longer lawfully held. SO15 are aware of this issue and are taking all reasonable steps to ensure NSDs are made only in respect of lawfully retained material. Nevertheless my Office has referred back a small number of cases of this type.

NSDS: 'MATERIAL' VERSUS 'INDIVIDUAL'

228. On a literal reading of the PoFA legislation, NSDs must be made in respect of biometric material, rather than for the person to which the material relates. In practice, therefore, PoFA prescribes that each time a new DNA sample and/or set of fingerprints is taken for an individual, a new NSD must be made in order to retain those records. This has proved less of an issue for Legacy Material as all existing holdings for individuals of CT interest were merged into a single NSD for each individual; however for New Material the situation is more problematic. For some cases where individuals have been detained or arrested on multiple occasions, there has been a requirement to make multiple NSDs for the same individual. This is another issue that the Government may wish to examine as part of the review of terrorism legislation ordered by the Prime Minister.

6. DELETION OF BIOMETRIC RECORDS

6.1 DNA SAMPLES

BACKGROUND

229. There are clear rules in PoFA as to when biometric samples should be deleted.[164] Whilst PoFA allows the police to take DNA samples from all persons arrested for a recordable offence these must, as a general rule, be destroyed once a profile has been derived and certainly within 6 months. These rules were a central new element introduced by the PoFA legislation to reflect Parliament's decision that the information contained in a person's DNA sample was so sensitive that once the police had derived a DNA profile for criminal justice purposes the sample should be destroyed. However, other legislation allows the police to keep DNA samples until a criminal investigation and allied disclosure arrangements are concluded. This is an exception under the Criminal Procedure and Investigations Act 1996 (known as the CPIA exception).

230. In my view the CPIA exception is just that, an 'exception' that allows the police to retain DNA samples for over 6 months in certain, very limited circumstances. If the CPIA exception were to be interpreted more widely, leading to the routine retention of samples by the police, then this would undermine the central element of PoFA on DNA sample retention. My predecessor therefore called for clearer guidance to be issued to the police on the use of the CPIA exception and Ministers agreed, in 2016, that *"further guidance on this issue would be beneficial"*[165] . It is disappointing to report that this guidance has still not been produced.

231. The majority of DNA samples taken for PACE or elimination purposes were passed last year to one of three Forensic Science Providers (FSPs) for profiling and the FSPs have the responsibility for deleting samples once a DNA profile has been obtained or for retaining it under the CPIA exception if requested to do so by the owning force. Since it is central to the regime introduced by PoFA that DNA samples should not be retained once a DNA profile has been derived I have monitored closely the deletion of DNA samples.

HAVE DNA SAMPLES BEEN APPROPRIATELY DESTROYED?

232. From my oversight activities and visits carried out to date I have found no reason to suspect that, apart from the use of CPIA exception, which is discussed in more detail 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.

---

[164] For details and discussion, see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at Section 4.1.

[165] Ibid at paragraph 181.

CPIA EXCEPTION

233. As discussed earlier, the general rule introduced by PoFA is that DNA samples should be deleted as soon as a DNA profile has been derived from them or no later than six months from the date they were taken, whichever is sooner. One exception to this general rule may be applied when a DNA sample is required for use in an ongoing investigation or if that DNA sample *"is, or may become, disclosable under the Criminal Procedure and Investigations Act 1996"*.[166] In such circumstances, the sample may be retained until it has fulfilled its intended use or, if the evidence may be challenged in court, until the conclusion of judicial proceedings and any subsequent appeal proceedings. [167]

234. Since January 2016, all DNA samples that are held under the CPIA exception beyond 6 months from the date they were taken, are required to be reviewed on a quarterly basis by the responsible police force. A record of that review process should therefore be available for audit purposes.

235. DNA samples which are retained under 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).

Since January 2016, all elimination samples have been subject to the same retention rules as those taken from individuals arrested for recordable offences.[168]

236. It is possible for 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 is clear that forces in fact do so. This may be because there is an underlying problem with the CPIA exception. The wording of the exception if taken literally to mean until all *possible* investigation and disclosure are completed, including, for example, a possible criminal cases review, could lead to all samples being retained because such possibilities are unpredictable. This would undermine the core PoFA principle of not retaining DNA samples.

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

[167] Further information about the development of the CPIA exception can be found at: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2014* at paragraphs 178-182.

[168] For further discussion of volunteer samples see: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016, 226-231.*

NUMBERS

237. The Forensic Information Database Service's DNA Unit (FINDS-DNA), have 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'. Those schedules can at best provide me with only an approximate picture of the position as regards the retention of samples under the CPIA exception as samples are retained and destroyed on a near constant rolling basis.

238. It should also be noted that the quarterly returns for 'in force' holdings received by FINDS-DNA are not complete as a significant number of forces have failed again in 2017 to consistently provide figures as requested. This situation is unsatisfactory because it does not allow either me or FINDS-SB to monitor PoFA compliance or to ascertain whether there is a national approach to the use of the CPIA exemption.

239. The last quarterly report received by my office gives the retention figures for DNA samples held under CPIA 'in force' and with FSPs as at 31 December 2017. These are set out below (Table 20).

TABLE 20: DNA samples held under CPIA (year ending 31 December 2017)

	Total	Held in Force[169]	Held by FSPs
Arrestee Samples	7,952	1,184	6,768
Elimination Samples	8,861	3,631	5,230

(Source: FINDS-DNA)

240. These figures have been giving me cause for some concern since they show that some forces are using the CPIA exception to routinely instruct FSPs to keep DNA samples whilst other forces are keeping much smaller numbers and deciding whether to do so on a case by case basis.

241. It has, further, come to my attention, through visits to forces and discussions with key stakeholders that forces are interpreting and applying the CPIA exception inconsistently. In the last 18 months, I have seen a rapid rise in the number of samples – both PACE arrestee

[169] The following police forces did not provide figures in December 2017 to FINDS-DNA of their 'in force' holdings of DNA samples held under CPIA: Bedfordshire, Humberside, West Yorkshire, North Yorkshire, South Yorkshire, Warwickshire, West Mercia, Durham and the MPS. The figures reported are therefore not fully reflective of the national picture in relation to 'in force' holdings of DNA samples. Moreover, 3 forces were unable to break down their holdings into arrestee and elimination samples (for a total of 134 samples)

and volunteer/elimination – held under this exception both 'in force' and with Forensic Service Providers. In addition, reviews of DNA samples, which have been held with Forensic Service Providers for over 18 months, have shown that the vast majority of B scrape samples (the second of two samples routinely taken by the police) retained under the CPIA exception have not been used for further/specialist analysis. It appears therefore that, at least for some police forces in England and Wales, routine and/or 'blanket' retention of large numbers of DNA samples under CPIA has become the norm. As a result of this situation very real questions have arisen as to whether Parliamentary intention that DNA samples be routinely destroyed is being undermined.

242. In the absence of the Home Office issuing guidance on the use of this exceptional retention power and given the concerns just described I wrote to all forces in December 2017 setting out my concerns and suggesting key principles in respect of the operation of the CPIA exception. See **Appendix D.**

243. I regard this letter as an interim measure until either the Home Office or FINDS-SB provide forces with guidance. The reasons why forces may want to keep samples need more consideration. If arrestee samples are being kept because the defence may require further analysis then this seems unnecessary since in such circumstances it would surely be in the interests of a defendant to provide another sample for analysis. If they are being kept because the B sample may be needed for separate analysis, for example in some rape cases a Y-STR analysis could be needed, then such cases are usually identifiable early in an investigation and either such analysis carried out within the permitted six month holding period or a CPIA exception applied until it is done.

244. There is a further problem of whether PoFA can be interpreted as meaning that once a profile has been derived then both samples should be destroyed, unless the CPIA exemption is applied, or whether the B sample may be retained until the end of the six month period in any event. In addition, to ensure PoFA compliance, and because further analysis of the B sample takes time, FSPs tend to destroy samples well before the six month deadline.

245. I will continue to monitor the use of the CPIA exception by forces, in particular in relation to whether they are taking case by case decisions as to when they need to retain a particular sample under the CPIA exception and whether they are keeping appropriate and timely records of the reasons for so doing. If guidance is issued I will also monitor compliance with the guidance.

6.2 DNA PROFILES AND FINGERPRINTS

246. Previous Reports discussed a number of problems with the proper deletion of DNA profiles and fingerprints as required by PoFA.

COPIES

247. The provisions governing the retention and use of copies of fingerprints and DNA match reports are contained in section 63Q of PACE (as amended by PoFA).

248. As regards copies of DNA profiles and fingerprints it remains the case that, apart from copy fingerprints that are being retained in the National Fingerprint Archive or in case files, I have no reason to suspect significant non-compliance with section 63Q of PACE.

249. None of the police forces 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 of hard copy fingerprints which should no longer be retained.

250. Following my predecessor's visits to police forces and to the National Fingerprint Archive various recommendations were made to the police, in 2015, as to how their processes and procedures might usefully be clarified and/or improved. I can report that all those recommendations have been acted upon and the Archive provides regular performance statistics on its operations to my Office on a quarterly basis.[170]

TABLE 21: Deletions from National Fingerprint Archive (Year ending 31 December 2017)

	All Forces 2016	All Forces 2017
Total PoFA deletion notifications received from IDENT1	**42,111**	**30,393**
Hardcopy records found and destroyed	7,281	2,301
No. of hardcopy records not held in National Collection	34,357	28,104
Requests received from other police forces where ten-print records were found and destroyed[171]	147	96

(Source: National Fingerprint Archive)

As is to be expected, the number of deletions of hardcopy fingerprint sets is reducing over time.

[170] Special thanks to Ruth Simmons, Archive Manager, for her help in preparing the relevant data.

[171] Where the National Fingerprint Archive holds a set of fingerprints in the National Collection on behalf of another police force.

6.3 DELETION OF POLICE RECORDS[172] ORDERED BY CHIEF OFFICERS

251. People whose biometrics are being lawfully retained by the police can apply for the 'early' deletion of their records from national police systems[173]. Previous Annual Reports drew attention to the very limited circumstances under which such an application could be made[174]. The Records Deletion Process (RDP) now allows individuals to make an application for deletion of their PNC record and associated biometrics in respect of out of court disposals, NFA disposals and non-conviction disposals issued in court[175] if they are able to evidence the 'grounds' for such a deletion. It must be noted, however, that it is still for the individual to make out the grounds – which in themselves remain somewhat limited - upon which they believe their record ought to be deleted and the decision as to whether to do so is entirely at the discretion of the Chief Officer (taking into account the aforementioned guidance). In the year ending 31 December 2017, 468 such deletions were ordered by Chief Officers (see Table 22 below). Whilst these figures are not directly comparable to those in my previous Annual Report[176] both the number of applications for deletion and the number of records approved for deletion appear to have increased, although it must be noted that these deletions still represent only a very small proportion of those records that are potentially eligible for deletion.

[172] The 'Record Deletion Process' (RDP) enables an individual to make an application for the removal of an arrest event from the PNC and the associated biometrics if held (in some cases biometrics may already have been deleted under the relevant PoFA provisions so the application relates only to the PNC record).

[173] 'Deletion of Records Held on National Police Systems (PNC/NDNAD/IDENT1)'

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430095/Record_Deletion_Process.pdf

[174] See: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at section 4.3.

[175] e.g. not guilty, withdrawn, discontinuance disposals.

[176] Previous deletions ordered were 233 (of 1,003 applications to delete) during the ***fiscal*** year 2015/16.

TABLE 22: Records Deletion Process (year ending 31 December 2017)

Total Applications received by ACRO Records Deletion Unit	Approved by Force	Rejected by Force	Rejected as ineligible by ACRO Records Deletion Unit	Pending with Force
1,648	468[177]	564	427[178]	171

(Source: ACRO Criminal Records Office – Records Deletion Unit)

[177] Of these 19 were approved for partial deletion. In those instances the applicant is seeking the deletion of more than one arrest event/offence from their record but the force approves the removal of one (or two etc) but not all events/offences sought for deletion.

[178] Of these 1648, 1203 were sent to forces. 427 were rejected due to ineligibility for the process and 18 await further information from the applicant (at the time of writing). Reasons for ineligibility include: no PNC record or record of event sought for deletion held on the PNC, court conviction sought for deletion, the applicant is the subject of a confirmed ongoing investigation or the applicant didn't respond to request for further information.

7. INTERNATIONAL EXCHANGES

7.1 INTERNATIONAL EXCHANGE OF BIOMETRICS

252. One aspect of my role is that of overseeing the sharing of biometric material internationally. The Home Office's International DNA Exchange Policy for the United Kingdom[179] 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."*

253. The international exchange of DNA profiles and associated demographic information is governed by the Home Office *International DNA Exchange Policy for the United Kingdom*. This guidance clearly sets out the parameters in which DNA exchanges can take place and details the nationally agreed processes and mechanisms for doing so. There is currently no equivalent Home Office policy for the international exchange of fingerprints and this apparent governance deficit has left those agencies responsible for the international exchange of such data to operate without a national government policy steer.

254. In the absence of a policy for international fingerprint exchanges my advice, as it was of the previous Commissioner, to those involved has been to mirror the processes in place for international DNA exchanges. The exchange policy for DNA is currently being redrafted to incorporate the international exchange of fingerprints. My Office has been sighted on those proposed changes and has been involved in discussions over how the two biometrics should be treated. The new policy, once agreed, should hopefully provide to those agencies involved in the international exchange of fingerprints a national policy steer which has to date been lacking.

255. A key issue in those discussions has been the extent to which international biometric exchanges should initially be anonymised, with the biographical detail associated with the biometric only shared if/when a match has been made. Existing guidance on the exchange of DNA profiles[180] has been that international exchanges should initially be anonymised until a link is established and only then should biographical information be exchanged. Given the lack of guidance for fingerprint exchanges, I have so far adopted the same approach to fingerprints as to DNA samples and profiles, as did my predecessor.

256. During the course of this year the practice of how international exchanges of DNA and fingerprints should be conducted has been challenged. The police, particularly the NCA and ACRO, have argued that the purpose for the international exchanges of DNA profiles and fingerprints is quite different. Their view is that DNA is primarily exchanged to see if a link between a crime scene stain and a known offender can be found and that initial exchanges

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

[180] DNA samples are rarely, if ever exchanged.

can reasonably be anonymised until a link is established, whilst fingerprint exchanges are primarily used to confirm identity and therefore require biographical details to be attached at the time of exchange. I am not convinced that this distinction can be easily made nor why it has the implication claimed.

257. If fingerprint exchanges were to be treated differently than DNA then that would be a significant policy decision, which seems to me a decision for Ministers. However, this divergence of opinion does again raise the issue of whether there ought to be comprehensive nationally agreed policy and guidance for the international exchange of both fingerprints and DNA, which clearly sets out the processes and considerations to be followed when exchanging both DNA and fingerprints internationally, whether that be that the two biometrics should be treated the same or differently. This does not simply mean issuing guidance about existing practice since for fingerprints the first step will involve agreeing on the content of the policy. This is becoming urgent as the number of different routes for international exchanges increases under the control of different parts of the UK policing structure and as there is a need to align with EU procedures to provide the basis for continuing exchange with European countries post-Brexit.

7.2 THE ROLES OF THE UKICB AND ACRO

258. The National Crime Agency (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, European Arrest Warrants and the case management of international enquiries. Except for matters relating to counter-terrorism, most requests for the international exchange of DNA profiles are channelled through the NCA. The NCA also deals with the international exchange of fingerprints for intelligence purposes.

259. ACRO Criminal Records Office is a national police unit created originally by the Association of Chief Police Officers (ACPO) but now responsible to ACPO's successor the National Police Chiefs' Council (NPCC). 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.

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

7.3 EXCHANGE OF FINGERPRINTS IN THE CONTEXT OF CONVICTION INFORMATION

EXCHANGE WITH EU MEMBER STATES

260. ACRO exchanges criminal conviction data with the other 27 EU member states under Framework Decision 2009/315/JHA. Exchanges of the fingerprints of EU and UK nationals take place in response to 'Requests' or 'Notifications'. [181]

EXCHANGES WITH NON-EU MEMBER STATES

261. 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 in response to Requests and Notifications and may again involve the exchange of fingerprints.

Table 23 below provides comparative figures in relation to EU and non-EU exchange requests.

TABLE 23: Fingerprint Exchanges (year ending 31 December 2017)

	EU Exchanges	Non-EU Exchanges
Requests in	315	2,201[182]
Requests out	19,897	8,861[183]
Notifications in	22	42
Notifications out	7,255[184]	8,727[185]

(Source: ACRO Criminal Records Office)

7.4 EXCHANGE OF DNA AND FINGERPRINTS FOR INTELLIGENCE PURPOSES

262. The international exchange of DNA and fingerprints for intelligence purposes is co-ordinated by the NCA, which houses the UK's 'Interpol hub'. ACRO provides the 'Requests In' Service to the NCA and therefore receives these requests directly from the NCA.

---

[181] For a detailed discussion of the mechanisms by which conviction information and fingerprints are exchanged between EU and non-EU member states see: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 282-289.

[182] Non EU requests in can include some EU requests as these all come directly from Interpol.

[183] Sent to Interpol and to the country.

[184] 7,255 were uploaded to Interpol with 5,055 of these also sent to the country directly.

[185] Sent to Interpol and to the country.

DNA SAMPLES

263. DNA samples are very rarely exchanged. The NCA 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.

No DNA samples were exchanged between 01 January 2017 and 31 December 2017.

DNA PROFILES

264. 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. Table 24 below provides the figures for inbound and outbound DNA Requests.

There are 4 types of DNA profile enquiry that are dealt with by the NCA.[186]

OUTBOUND SUBJECT PROFILES

265. DNA profiles should always be anonymised before being sent to another country for searching. The DNA profile of a known individual is sent abroad only with the express approval of the Chief Officer of the law enforcement agency that took the DNA sample and the FINDS-SB, following a full risk assessment.[187]

INBOUND SUBJECT PROFILES

266. DNA subject profiles are received from abroad and sent to FINDS-DNA for searching against the NDNAD. The Home Office Policy details the criteria under which searches will be authorised.[188]

OUTBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

267. 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

[186] 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.

[187] See further *Home Office International DNA Exchange Policy for the United Kingdom*, at paragraph 7.1.2.

[188] Ibid at paragraphs 7.1.1.

force investigating the crime. The Home Office Policy details the criteria under which DNA profiles will be released from the NDNAD for searching.[189]

INBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

268. DNA crime scene profiles or unidentified body profiles may be received from abroad. The Home Office Policy states that, absent specific authorisation by FINDS-SB, 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'.[190] 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*".

TABLE 24: DNA Profile Enquiries (year ending 31 December 2017)

	Outgoing from UK			Inbound to UK		
DNA Type	**Total**	**Searches concluded**	**Positive/ Potential Match**	**Total**	**Searches concluded**	**Positive/ Potential Match**
DNA Samples	0	0	0	0	0	0
DNA Subject Profiles[191]	23	17	1	107	71	9
Missing Persons	16	14	1	75	52	7
DNA Crime Scene profiles[192]	166	156	13	619	484	34
Unidentified Bodies	14	12	1	97	83	6

(Source: NCA)

[189] Ibid at paragraphs 7.2.2.

[190] It seems that, as a general rule, the NCA 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.

[191] (figure includes missing persons)

[192] (figure includes unidentified bodies)

FINGERPRINTS AND FINGER-MARKS

269. There are 4 types of fingerprint enquiry dealt with by the NCA. In the absence of a national Home Office policy for the international exchange of fingerprints, the NCA has produced its own policy which largely mirrors the criteria set out in the Home Office International Exchange Policy for the UK with an additional provision for the exchange of fingerprints for the purposes of identification.

Table 26 below provides the figures for inbound and outbound Fingerprint Requests.

OUTBOUND FINGERPRINTS

270. 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 or because the individual in question is a convicted sex offender who intends to travel to another country.

271. Any force which wants fingerprints sent abroad must explain to the NCA why they think that there is a link to the specific country or countries to which the prints are to be sent.

INBOUND FINGERPRINTS

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

OUTBOUND CRIME SCENE FINGER-MARKS

273. Requests to send crime scene finger-marks to other countries are rarely made, although work is ongoing by the NCA through their Liaison Officers to educate regional forces as to the investigative benefits of international searching.

INBOUND CRIME SCENE FINGERMARKS

274. 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.[193]

[193] However, as with inbound crime scene profiles, it seems that the NCA will also agree to the searching of an inbound crime scene finger-mark if the relevant offence falls within the ambit of a list of serious offences which has been approved by the Home Secretary or where fingerprints are exchanged to confirm identity of an individual.

TABLE 25: Inbound and Outbound Fingerprint Requests (year ending 31 December 2017)

	Outgoing from UK			Inbound to UK		
Fingerprint Type	**Total**	**Searches Completed**	**Positive/ Potential Match**	**Total**	**Searches Completed**	**Positive/ Potential Match**
Ten-print sets	799	799	190	1969	1969	62
Crime scene finger marks	2	2	1	108	108	0

(Source: NCA)

DIP-SAMPLING

275. My Head of Office has carried one dip-sampling exercises this year; in January 2017.

276. During a visit to the offices of the NCA in January 2017 my Head of Office dip-sampled 21 cases, in 7 of which DNA searches were conducted for offences which were not listed on the UK qualifying offences list and prior approval had not been sought from FINDS-SB. These cases had been identified by NCA through its internal audit processes as not in accordance with the Home Office Policy prior to dip-sampling.

POTENTIAL 'BIOMETRIC BREACHES

277. In response to the issues identified above, actions have been taken to address the errors identified and also in order to prevent similar issues in the future:

- New internal guidance has been drafted and published in respect of fingerprints and DNA;
- Additional training has been provided for teams who deal with DNA international searches in order to highlight the new rules; and
- More frequent internal quality auditing has taken place to identify issues and mitigate their consequences.

278. I am grateful to the staff at the NCA for bringing these cases to my attention and more generally for their assistance over the last year.

EUROPEAN ARREST WARRANTS

279. The NCA 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).

280. 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[194] and is responsible for recording all requests received through the Sirene system. All EAW requests, whether or not they have a UK connection, are now recorded, which has resulted in a higher number of recorded requests since 2014/15 than in previous years.

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

282. In the fiscal year 2016-17, 345 EAW requests were made by the UK and 16,598 EAW requests were received by it. Table 26 gives a yearly comparison since 2013.

283. **TABLE 26: EAW Requests by fiscal year (2013/14 – 2016/17)**[195]

	2013/14	2014/15	2015/16	2016/17
Requests from the UK	230	223	241	345
Requests into the UK	7,881	12,134	14,279	16,598

7.5 INTERNATIONAL CONVICTION INFORMATION

LOADING NON-UK CONVICTIONS TO THE PNC

284. 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. Notably,

- 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;

[194] '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).

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

- 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
- convictions will only be treated as being of that type if they are for offences that fall within the scope of a list of serious offences which has been approved by the Home Secretary.[196]

Indeed 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 scope of that list.[197]

285. In the 2015 Annual Report, my predecessor explained that that list, which has never been published, leaves scope for the exercise of judgment and/or discretion in a variety of circumstances and that it would be desirable that guidance be issued to ensure that such discretion is applied in a consistent and appropriate manner.

286. Although it was understood that relevant guidance would be finalised within weeks of that Report, no such document has been published. Nevertheless, when I visited ACRO in October 2016, my Head of Office and I dip-sampled a selection of decisions in respect of the exercise of such discretion. There was nothing about those cases which caused either of us any concern.

UK NATIONALS WHO HAVE OFFENDED ABROAD

287. 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.[198] 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.[199] DNA information is rarely (if ever) received in connection with such convictions but fingerprints sometimes are. In those circumstances the fingerprints will be loaded to, and retained on, IDENT1.

---

[196] See Appendix B of this Report. Also see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 76-78.

[197] 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.

[198] 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.

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

7.6 INTERNATIONAL EXCHANGES AND BREXIT

288. Some of the international exchanges explained above depend on EU agreements. If and how these will change in a post-Brexit world remains to be seen, although the Government has made clear that it regards these as in the mutual interest to maintain. This position has been repeated recently by the Prime Minister in her speech in Munich on 17th February 2018[200] and by bringing the EU's new General Data Protection Regulations (GDPR) into UK law we will, at least for the present, share a common approach to data.

289. Not all international exchanges, however, depend on EU arrangements and post-Brexit, the UK will remain within broader exchange mechanisms such as Interpol.

290. Not only has the Government made clear that it intends to try and continue its membership of EU data exchange mechanisms but, as a sign of this, the Government has continued to work towards the implementation of DNA, fingerprint and vehicle number plate information exchange via the Prüm Mechanism.

7.7 PRÜM

291. The Prüm Council Decisions of 2008[201] allow for the reciprocal searching of DNA and fingerprint databases within the EU on an anonymised 'hit/no hit' basis. As was explained in the 2014 Annual Report[202], those Decisions were subject to the UK's opt-out under Protocol 36 of the Lisbon Treaty.

292. However, in December 2015[203] it was decided that the UK would rejoin the Prüm exchange mechanisms on the basis that proposed safeguards will be brought into force. Those safeguards were agreed by Parliament and include conditions to the effect:

- that only the DNA profiles and fingerprints of persons convicted of a crime will be made available for searching by other EU Member States;
- 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;
- that such information will only be released in respect of a minor if a formal request for Mutual Legal Assistance has been made; and

---

[200] https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018

[201] 2008/615/JHA and 2008/616/JHA

[202] (at paragraphs 308-309)

[203] 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.

- that the operation of the system will be overseen by an independent Prüm Oversight Board.

293. Following the successful DNA pilot scheme in 2015, an interim solution for commencing regular DNA exchanges via the Prüm exchange mechanism using an MPS owned CODIS[204] database has been agreed by Ministers and the Government hopes that the exchanges will start this year. In addition, the first phase of the UK fingerprint exchange solution via Prüm is being developed in partnership with Germany. Ministers have committed to exchanging DNA, fingerprint and vehicle registration data with at least one member state this year. However, joining Prüm exchanges will involve the UK meeting the technical requirements of the EU, demonstrating that the exchange mechanisms work and being accepted by the remaining EU member states.

294. Both I and the Information Commissioner will have a role in overseeing and auditing Prüm exchanges.[205] What form that will take is not yet clear since the focus so far has been on gaining EU approval for the Prüm exchange to begin. I shall be concerned to ensure that, since the Prüm DNA exchanges will use an MPS database, proper governance arrangements are in place[206]. If the UK joins the Prüm exchange then the initial result will be that international exchanges will be split between three policing agencies[207] and begs the question as to whether this is the best arrangement for the future.

7.8 FURTHER PROPOSED INTERNATIONAL EXCHANGES

295. The Counter Terrorism Command (SO15) of the MPS is proposing that an extension of their DNA international exchange process should be put in place for counter terrorism purposes so that the UK can share biometrically enabled watch lists with partner countries. Since this is currently under discussion it is not possible to be more precise at present. I have made clear so far during those discussions that:

a. exchanges should fit within any new policy which emerges on how biometric data should be exchanged internationally in the future – see section 7.1 above.

b. I must be able to exercise my statutory obligation to report on the retention *and* use of biometric material for counter-terrorism purposes. I need to be certain that appropriate data, access and knowledge of the decision making processes for these international exchanges is available to me. This needs to be agreed because the

[204] (Combined DNA Index System)

[205] See 7.7 of last year's Report.

[206] HOB are building the capability for Prüm fingerprint exchanges within IDENT1.

[207] The NCA, MPS and ACRO.

governance will necessarily and properly be complex ranging from some Ministerial decision making to that by a SO15 Inspector.

296. I will report further on this matter in my next Annual Report or earlier in a Report to the Home Secretary[208] if I feel that appropriate.

[208] Under s21(2) of PoFA.

8. FUTURE BIOMETRIC CHALLENGES

8.1 TECHNICAL CHANGE AND NEW CHALLENGES

297. The challenge for the Government to keep citizens safe has, in some areas, been increasing. Traditionally measured crime has gone down significantly since the late 1990s[209] but at the same time there has been a rise in new forms of crime, such as internet-based fraud or sexual offending facilitated by the use of the internet and social media. Over the same period the risk of internationally inspired terrorist attacks in this country has increased.

298. Technological change has provided new opportunities for the commission of crime and for offenders to hide their activity or identity. However, the same technological changes have also provided powerful new tools to identify and respond to such threats. Whilst the state may have powerful new tools available to it, if misused, they could undermine the very liberties and civil society that it is seeking to protect. It was in this context that Parliament passed the Protection of Freedoms Act (PoFA), in 2012, to strike a balance such that the police were given the tools to respond to these new challenges whilst ensuring that those tools did not interfere in personal liberty any more than was necessary for the protection of the public interest.

299. PoFA only controls the police use of DNA and fingerprints (and footwear impressions) in criminal and national security cases; however, previous reports drew attention to the development and deployment by the police and others of new biometric technologies.

300. Last year's Report referred to the imminent publication, by the Home Office, of a Review of the Retention and Use of Custody Images and a Biometrics Strategy since both had been promised to the House of Commons Science and Technology Select Committee in December 2014.[210] The *Review of the Use and Retention of Custody Images* was published on 24th February 2017.[211] At the time of writing, the Biometric Strategy is still awaited but the Minister responsible for biometric policy in the Home Office, Baroness Williams, recently

---

[209] Although recently police recorded crime has been increasing the Crime Survey does not record such an increase. It is therefore difficult at present to know whether there is actually an increase but that the nature of the offences that are increasing are not best measured by the Survey or whether the Survey does measure the increase but that it only does so with a lag effect. Regardless of the above more police recorded crime will increase the amount of biometric work that needs to be done by the police and perhaps, consequently, the number of applications to me to retain biometrics.

[210] Response to the Science & Technology report: *Forensic Science Strategy: Government Response to the Committee's Fourth Report of the Session 2016-17* which says *"The [Biometrics Strategy] is in the final stages of completion and will be published shortly."*

[211] https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

promised the House of Commons Science & Technology Committee that it would be published in June this year.

301. The development of new technologies has thrown up four important challenges for any future use of data to authentically identify individuals or to link individuals to forensic evidence found at crime scenes or on the person of a victim. These four challenges are:

- The development of second generation biometrics, beyond fingerprints and DNA, to a stage of maturity where potentially they could be deployed by the police.
- The development of new, multi-user, biometrics data platforms.
- The emergence of new algorithms, using machine learning, in programmes claiming to provide biometric 'matches'.
- The development of sociometrics – that is analysis of large data sets to identify regular patterns of social behaviour that could be used to identify individuals in the same way as do biometrics.

8.2 SECOND GENERATION BIOMETRICS

302. The only biometrics routinely in use by the police at the time of the passing of PoFA were DNA and fingerprints, as the use of these had already developed to a level of maturity such that they were able to be deployed by the police reliably and on a large scale. Consequently, PoFA only controls the police use of DNA and fingerprints (and footwear impressions) even though other biometrics which could be of use to the police had already been identified and were under development. However, at the time PoFA was passed the general scientific opinion was that these second generation biometrics were not at a state of maturity such that they could be deployed by the police or other public agencies. Over the last six years these new biometrics have developed considerably and the ability of software systems to produce biometric 'matches' has improved rapidly. In some cases second generation biometrics, such as facial image matching, are now being deployed by the police, although their use should still be limited by the current technical capabilities.

303. Given that PoFA is not generic legislation covering all biometrics used by the police, the use by the police of these second generation biometrics is not currently governed by any specific legislation, other than general data protection legislation, and only by regulations drawn up by the police themselves such as the Management of Police Information principles (MOPI) drawn up by the College of Policing. It is therefore the case that technical development and deployment is running ahead of legislation, which is why the Home Office's promised biometric strategy is urgently needed.

304. Of all the second generation biometrics that are being developed the one that has been most widely deployed by the police has been facial imaging. The use of facial custody

photographs (mug shots) is as old as photography itself. The more recent development of digital images has opened up the possibility of creating and maintaining large databases of images. The use of image matching software and this extension into new technology was a natural development for the police. By coincidence, the Bichard Report[212] after the Soham murders recommended the creation of a new database for the sharing of police intelligence: the Police National Database (PND).[213] It is this national database that, under the leadership of the Chief Constable of Durham Constabulary (Mike Barton), has subsequently been used to store digital custody images which can be searched using image matching software.

305. The Review of the Use and Retention of Custody Images[214] published by the Home Office last year arose, at least in part, from the need by the Government to respond to a 2012[215] court judgment. This judgment was critical of the governance arrangements for custody images then in place and in particular that the retention regime was not proportionate in its treatment of unconvicted persons to the extent that it was unlawful. The Review attempted to address the issue of proportionality by introducing a process by which those not convicted of an offence can apply to the police to have their facial images deleted and introduced a presumption of deletion, but the police have the discretion to refuse such a request. Baroness Williams of Trafford was recently asked by the Science and Technology Select Committee to write to them with exact figures as to the numbers of such applications made to police forces for deletion of custody images. Whether the limited changes introduced by the Review will be sufficient in the face of any future legal challenge remains to be seen[216] but a case currently waiting judgment by the European Court of Human Rights may provide further guidance and clarification on this issue.[217]

306. In July 2016, in answer to a Parliamentary question from Lord Scriven, it was reported that were 19 million facial images on the Police National Database (PND) 16,644,143 of which had been enrolled in the facial image recognition gallery and were searchable using facial recognition software.[218] It was not clear how many of those images were duplicate images or how many related to unconvicted persons. In addition, not all police forces uploaded images to PND, including the MPS who hold their own extensive collection of facial

[212] http://dera.ioe.ac.uk/6394/1/report.pdf

[213] http://www.safeguardingchildrenea.co.uk/resources/the-bichard-inquiry-report/

[214] https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

[215] *R(RMC and FJ) v Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin)

[216] See my comments at the time: https://www.gov.uk/government/news/response-to-the-home-office-review-of-the-retention-and-use-of-custody-images

[217] Fergus Gaughran and the Chief Constable of the Police Service of Northern Ireland and the Secretary of State for the Home Department UKSC 2013/0090.

[218] HL1211 and HL1213 at www.parliament.uk/business/publications/written-questions-answers/

images[219]. More recent information provided to me in January 2018 is that a total of 21 million images are held on PND but of those only 12.5 million are within the facial image recognition gallery. The remainder of the images are apparently either non-facial images, such as tattoos or scars, or are low quality facial images (>10mgb) which are not deemed suitable to be included in the facial recognition gallery. The Metropolitan Police have also started uploading images to PND but only of convicted persons. The gallery is not used automatically to match against people in public places. Rather it is used to search for matches against unidentified facial images found in the course of a police investigation for example, on CCTV footage or a mobile phone. It may be used to search for suspects, victims or vulnerable people.[220] Information about these custody image holdings and their use has not been routinely made public by the police or the Home Office. I am puzzled by this since providing this limited transparency would, in my view, help build the legitimacy the police need to develop their use of facial images and other second generation biometrics.

307. Separately from the use of custody images some facial images stored by the police are being experimented with to ascertain whether it is possible to use these images to identify individuals in public places. The Home Office's Review of Custody Images did not cover this quite different use of facial images and this remains outside the MOPI principles put in place as a result of the Review. In practice what this means is that DNA and fingerprints have clear rules as regard their taking, retention and use as decided by Parliament (in PoFA) and with independent oversight of compliance but custody images can be taken on arrest and retained regardless of the legal outcome and can be retained until the police carry out a review after six years or until the subject successfully applies to a Chief Officer for deletion under a process put in place by the College of Policing.[221] For other use of facial images and other second generation biometrics there are no specific rules on retention but their taking must be lawful and sometimes their retention may be forbidden.[222]

308. Both the Metropolitan Police and South Wales Police are currently running trials attempting to match some retained facial images with people in public places. I have written to both police forces saying that I consider that such trials may be acceptable as a way of exploring whether facial image matching technology can be used successfully in such an environment. Whilst there is good evidence of the matching capabilities of different facial matching software products in reasonably controlled use environments, such as matching custody images or passports at airports, there is little evidence as yet about matching for this much

[219] I understand that the MPS have now loaded around 60,000 images of convicted people to the PND.

[220] Information provided by Home Office PND.

[221] //www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/

[222] For example, West Yorkshire Police, as part of the HOB programme, have recently been using mobile fingerprint scanners to check any recorded previous police contact upon stop and can do so under certain condition under PACE 61(6A) but may not then retain the scanned fingerprint image.

more challenging use.[223] Furthermore, what needs to be understood is not just the matching capabilities of the software products but what kind of management and decision making system is required for such a police use in the criminal justice system. In this context trials can be justified if they have been carefully designed to provide new evidence to fill these gaps in knowledge and the results of the trials are published and externally peer reviewed. Crucially, there needs to be transparency about the reason for conducting trials and, in particular, what safeguards are built in to protect personal biometric data as well as consideration of the proportionality of its use.[224] However, using facial images operationally to search in crowds is more difficult to justify given the present technical limitations of such a use. So far transparency about the MPS trial has been partial, and has led to public criticism.[225] The South Wales trial has been more widely publicised both prior to and at the events where the trial has taken place and has, in general, been better received by the public. This illustrates that any future police use of biometric data will need to be transparent if it is to carry public trust in addition, of course, to compliance with any legislative or governance requirements.

309. The Home Office's Biometrics Programme (HOB), in conjunction with its sister programme the National Law Enforcement Database Programme (NLEDS), will provide a new national data platform for the storage of facial images and a new facial image matching system is to be procured. This new facial image matching system will be chosen for the utility to be optimised for the matching of custody images. That system may not be optimum for other uses, such as matching capability of 'one to many' in public places. However, HOB will be able to use more than one software system on its platforms in order to maximise optimisation for different uses. The new systems will improve on the current PND facial management systems and hopefully mean that the police will be able to implement and manage whatever retention and deletion rules are put in place in future for the governance of facial images. On current timescales it is envisaged that this will become operational during 2020.

310. Facial images are just the first of the new, second generation biometrics to be used operationally by the police but they are already experimenting with others, such as voice recognition. The use by the police of other biometrics may well be in the public interest and improve public safety but the fact is that neither governance nor legislation has kept up with the growth of these second generation biometrics. Lack of governance is leaving a worrying vacuum which the police tell me is making their experiments with new biometrics more

[223] See the testing programme of NIST: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

[224]The Information Commissioner has written to the Chief Constables of Durham and Dorset (as the leads on PND and biometrics) amongst other things making similar points. ICO letter, 30th November 2017.

[225] See e.g. https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/undemocratic-unlawful-and-discriminatory-civil-liberties-and-race

difficult and uncertain and so risks undermining public confidence in policing. Furthermore, lack of clarity about future governance arrangements for new biometrics may actually impede growth, since it is less costly to develop operational systems within a known governance structure than to have to adapt existing systems to take account of governance rules developed later.

311. More broadly, the police's involvement in the development of new technology such as second generation biometrics is not always organised or systematic. Our system of policing depends on Chief Constables having operational autonomy to ensure that policing decisions reflect the rule of law absent any other considerations. However, this autonomy is often interpreted much more broadly to mean that each force is free to experiment or introduce new technology as they see fit. Whilst the National Police Chief's Council (NPCC) can try and coordinate such developments, as it is doing through the Transforming Forensics Programme, it cannot enforce uniform adoption of shared technical solutions across the police service. This situation of force autonomy in developing technical solutions has had the advantage of allowing innovation and experiment but there is then not a strong mechanism for evaluation and deciding whether an experiment should be adopted by the other forces. We have seen the result of this in the case of the development and use of facial images where scientific leadership by one Chief Constable developed the use of custody images, which then drifted gradually into a partial national system. This is an odd way to develop new technical capabilities in policing. The police service needs to agree a common framework for the development, testing, evaluation and mutual implementation of new technologies. This is necessary if the service is going to keep ahead of new technology and be in a position to decide, on the basis of empirical evidence, how useful a particular technology will be for policing and, additionally, whether national deployment is in the public interest and is cost-effective. The same evidence will also be needed to persuade the public of the acceptability of such a decision.

8.4 NEW HOME OFFICE BIOMETRICS DATA PLATFORMS

312. When PoFA was passed into law it made no mention of 'databases' although their existence was assumed in the rules about retention or deletion; presumably from a database. At any rate PoFA acknowledged the National DNA Database by giving statutory existence to the then National DNA Database Strategy Board. As reported last year the Strategy Board's remit has been expanded to cover the fingerprint and footwear databases and it has now been re-named the Forensic Information National Databases Strategy Board (FINDS-SB).

313. PoFA governance applies to those defined in the Act as law enforcement agencies and therefore applies to the retention and use of DNA and fingerprints by those agencies. Both DNA profiles and fingerprints are held on national databases but PoFA is silent as to who should have access to the databases and under what conditions. I have reported earlier in this Report on the MoD access to IDENT1 outside the PoFA regulation. The police and UK

Visas and Immigration can search into each others' fingerprint databases (IDENT1 and IABS) but can neither delete nor add data to the other and do so on the basis of immigration legislation.[226] Conversely, the new Home Office Biometrics (HOB) data platforms, which are scheduled to become partially operational by 2020, are designed to potentially hold the databases belonging to a number of different government agencies but at present there are no governance rules about access and use to the different databases. [227] The example of MoD's access to IDENT1 illustrates that governance is very much needed to regulate access. It is worrying that these data platforms may go into operational use without this issue being addressed. The Home Office needs to acknowledge that their new, multi-user data platforms will need a clear governance structure and rules about who should have access to what and for what purposes. Furthermore, whether the regulation of access and use of the databases within these multi-database platforms can continue to be dealt with by regulations relating separately to each data using agency or will need pan-government regulation needs to be decided. Whether such control can be adequately provided by internal governance or will need legislative enactment also needs to be examined and addressed in the forthcoming Biometrics Strategy.

8.5 NEW BIOMETRIC ALGORITHMS

314. Any biometric used for policing will have the common characteristics of the digital coding of the biometric attribute, a database holding the biometric attribute and an algorithm designed to search the database and identify possible similarities. How well these technologies work operationally will depend on the quality of the data collected, how the matching algorithm works and the statistical probabilities behind the algorithm, but also the way in which this process is managed, interpreted and used in investigations and, ultimately, prosecutions. It is this whole system that underwrites the quality and reliability of the police use of biometrics. Failure to control and manage or understand any part of the system may lead to false 'matches' being claimed and may run the risk of wrongful convictions. Such a failure would damage public confidence in the criminal justice process.[228]

315. Until recently the algorithms used to identify possible matches in biometric databases were essentially the mechanisation of a pre-existing process of human decision making. However, we are now seeing the emergence of new algorithms that use machine learning or neural networks (often referred to as artificial intelligence or 'AI') to improve performance, potentially beyond that achieved by human analysis. Such new algorithms are already being

[226] See: Biometrics Commissioner Annual Report, 2014 paras 320-323.

[227] Although HOB have been involved in producing Privacy Impact Assessments in relation to some of the developments.

[228] The same point has recently also been made by the Forensic Science Regulator – see *Forensic Science Regulator: Annual Report 2016-17.*

used to develop facial matching and are being experiment with for other biometrics. Some currently available commercial biometric software now uses machine learning to improve analytic ability. The use of machine learning is an important development that is likely to improve the matching ability of biometric software. In the last decade we have seen significant improvements in biometric software in some areas, such as facial recognition, but these new algorithms may increase the pace of improvement.

316. These algorithm improvements are to be welcomed but the new algorithms do have a problem. The nature of machine learning is that once the software is initially programmed it then develops and changes as it indentifies patterns in the data sets offered to it, preferably with as much data as possible for the particular application. In this way it is often said that the software 'learns', although this is only the learning of pattern regularity rather than understanding. What the software has 'learned' however is not visible to its originator and indeed is a constantly ongoing process. This means that it is difficult, if not impossible, to describe how that software is determining possible matches; often referred to as the 'Black Box Problem' because it runs the danger of black box modelling, unchecked by human intervention, becoming the basis for decision making.[229] This scientific problem raises issues for ethics and governance since transparency, and therefore accountability, can be difficult if not impossible to achieve.

317. The 'Black Box Problem' also raises the practical issue of what reliance can be placed on such systems in judicial decision making. The standard procedure in Common Law criminal trials is that the defence should be able to challenge evidence put forward by the prosecution. However, if the prosecution is relying on the evidence of matches from software using these new algorithms then they will not know on what basis that match is claimed and, by the same logic, the defence will be unable to challenge the evidence, except, of course, in this general sense of pointing to the lack of intelligible evidence. In reality, courts have tended to rely on expert opinion to help them judge cases where the understanding of evidence may be difficult. Some have suggested that perhaps software could be frozen at one point in time and its 'matching' logic examined and described. However, machine learning, as already explained, is dynamic and such a description would become out of date very quickly afterwards. Others have suggested that the statistical probability of a 'match' being true could be calculated as the basis for expert evidence but again the dynamic nature of machine learning will leave that probability open to challenge. The work currently going on between the Royal Society, the Royal Society of Edinburgh and the judiciary, led by Lord Hughes may address this problem since it is designed to guide how evidence of this kind is presented and to ensure it is transparent and reflects general scientific opinion.[230]

---

[229] See e.g.: Grindrod, P; *Beyond privacy and exposure: ethical issues within citizen-facing analytics*, Philosophical; Transactions of the Royal Society A, November, 2016.

[230] See: ://royalsociety.org/news/2017/11/royal-society-launches-courtroom-science-primers/

318. There is some evidence that these new software systems may have biases in their ability to identify matches correctly. The testing of facial image software carried out by National Institute of Standards & Technology (NIST) in the USA[231] has found such biases. Why these biases are happening is a matter of some scientific dispute. Theories range from (unconscious) biases built into the original programming then further magnified, or the product of biased data sets being used as the basis for machine learning but these do not seem to fully explain the pattern of biases that have been found. At present we know that there are biases which vary between systems and that this needs to be clearly understood and allowed for in police use of such software in criminal investigation.[232]

319. It is sometimes said that matching based on such machine learning software will only be used for intelligence purposes and will not be used evidentially unless an additional process of human decision making confirming a claimed match has been undertaken. This answer, however, just pushes the problem further back in the process when the veracity of intelligence evidence will need to be judged and the danger that human decision making will be captured by technological authority.

8.6 TRANSFORMATIVE DATA USE

320. The use of biometrics is just one example of the very significant police use of data. Furthermore, it seems likely that police use of data, including but not limited to biometric data, will become an increasingly common and widespread. The Home Office is also working to develop the broader use of data analytics.

321. All of us leave records of our activities across cyberspace, public and private databases and in public spaces which, if analysed holistically, provide multiple ways of checking identity, modelling the patterns of our social behaviour, collecting or inferring our attitudes and recording our activities, movements and decisions. These records, taken as a whole, are referred to as sociometrics and may well be useful for future policing. Perhaps therefore to biometrics we should now add sociometrics.[233] Whilst I find it useful to distinguish between sociometrics and biometrics, the General Data Regulation (GDPR) of the EU and soon to be law in the UK does not make such a distinction regarding both kinds of identifiers as 'biometrics':

---

[231] See: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

[232] For a discussion of these issues see e.g. B.D. Mittelstadt, et al: *The Ethics of Algorithms: Mapping the Debate. Big Data & Society*, July-December 2016: 1-21.

[233] All manner of new analytic approaches are being used, such as agent-based modelling and numerical simulations (often borrowed from analysis in physics) to develop a computational social science. See e.g: J Borge-Holthoefer et al eds, (2016**):** *At the Crossroads: Lessons and Challenges in Computational Social Science,* Lausanne: Frontiers Media.

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; (GDPR Article 4(14)).

322. We are already familiar with big tech companies using data analytics to enlarge their businesses and, due to our regular use of their platforms, they have amassed very large, useful databases about our behaviour. Government also holds numerous and large databases which often contain very sensitive and private information about us. Until recently the value that could be gained from analysing data from large datasets or across databases was limited by the difficulties of large scale data analysis and of analysis across databases with different histories and architectures. However, all this is now changing. Modern computing has made analysis of very large data sets realistic and although still by no means as easy as often presented analysis across data sets is increasingly attainable. Furthermore, the re-development of data platforms is moving from being agency specific to generic (as we have seen in the HOB programme) so making general data analytics easier in the future.

8.7 FUTURE STATE USE OF DATA

323. Much of the aforementioned change is happening as technical modernisation without much public debate about the wider implications, the need for cross-government governance or how the balance between public benefit and privacy should be struck. It is the same question that PoFA sought to address for the much more limited issue of the use (of then) two biometric databases held by the police. The new EU General Data Protection Regulations (GDPR) and the Data Protection Bill currently going through Parliament will, however, provide the background for any future regulation of new biometrics or sociometrics.

324. The new data protection legislation builds on and strengthens individual rights. The Information Commission will also have greater powers to ensure compliance.

325. The Data Protection Bill has specific sections referring to law enforcement and to security and counter-terrorism which are based on six principles, namely:

i) Data processing should be fair and lawful;

ii) the purpose should be clear and legitimate;

iii) personal data should be relevant and not excessive;

iv) should be accurate and up to date;

v) kept no longer than is necessary; and

vi) processed in a secure manner.

326. The new Data Protection Act will apply to the police use of biometric material in addition to the specific requirements of PoFA. This means that any new governance or legal framework for the police use of biometrics beyond fingerprints and DNA will have to start with the requirements of this new legislation. However, when Parliament regulated the police use of DNA and fingerprints in PoFA it laid down requirements in addition to the then existing data protection requirements. One assumes that this was because it was felt that personal biometric material was especially sensitive and that its use by the police needed clear additional regulation if such a use was to carry public confidence and that Parliament was the right body to set out that regulation in legislation. In addition, of course, the Government was responding to the finding of the European Court of Human Rights[234] that previous legislation in relation to the retention and use of biometric material by the police was not proportionate.

327. PoFA does not start with a statement of principles, unlike the new data protection legislation, but nevertheless principles can be drawn from PoFA which often mirror those in the new data protection legislation, such as:

    a. That the holding of individual biometric information should be limited to that strictly necessary in order to achieve the determined public benefit. For example, in PoFA the public holding of DNA information was limited, in most circumstances, to profiles (its numerical encoding) as this was deemed to be adequate for law enforcement purposes and because DNA samples, if kept, could be used to derive further sensitive personal information.

    b. That for each use of biometric information the balance between public benefit and individual privacy (proportionality) should be decided by Parliament. By extension, deciding what is proportionate should not be left to those who seek to benefit from the use of the biometric.

    c. That the balance decided upon by Parliament is best implemented in law to express the will of Parliament and ensure legitimacy.

    d. That legitimacy will be further strengthened by independent oversight and reporting so that the public and Parliament are reassured as to compliance.

    e. That the use of biometrics by the state must carry public trust.

328. That trust will be fostered when there is clear and transparent governance of biometric use and its development which is discussed and challenged in public fora, and which is judicable.

[234] S and Marper v United Kingdom (2008) 48 ECHR 1169

329. It is for Parliament to decide whether these principles, used in PoFA, should also be used to inform any further legislation on the use of biometrics in addition to those of the new data protection legislation.[235]

330. The pace of development of new technologies which are either already or likely to be used operationally by the police is simply outpacing the speed at which Government is responding and, if thought appropriate, legislating. The Government of Scotland has grasped this problem and set up an independent advisory group last autumn which has already reported to the Government and whose recommendations have just been published as the Report of the Independent Advisory Group on the Use of Biometric Data in Scotland.[236] Whilst the legislative framework governing the police use of DNA and fingerprints in Scotland is different from that in England and Wales nevertheless the new problems that the Report seeks to address are common across the UK and indeed in many other countries. The Report is intended to generate a wider debate in Scotland about the use of any biometric data for policing and other public protection purposes and no doubt that will influence public discussion elsewhere in the UK. The Report's recommendations are bound to be of interest to the Home Office as it finalises its promised biometrics strategy for publication later this year and certainly to Parliament and the ongoing discussions by both the Science & Technology and Home Affairs Select Committees.

331. Given my remit I have limited my comments to the police use of future biometric data or its use in conjunction with other data analytics. However, there is a much larger issue of Government use of such data more generally and also the private sector's use of data and the interaction between the two. There is a growing public debate about how far new data technologies need to be governed by legislation. This not simply a negative reaction to new technology. There are clear benefits that we have and can gain from these technologies but as with any technological development it does not obviate the need to decide where the public good lies. That is the essential question of politics and should frame the application of new technologies not be driven by it.

[235] Other factors that might be considered in any future legislation were discussed in last year's Report at 8.8.

[236] http://www.gov.scot/Publications/2018/03/9437

APPENDIX A

THE NEW BIOMETRIC REGIME UNDER PACE

1. The relevant statutory provisions introduced by PoFA inserted sections 63D to 63U and 65B of PACE and amended sections 65 and 65A.

DNA SAMPLES

2. 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 taken. That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.

PROFILES AND FINGERPRINTS[237]

CONCLUSION OF THE INVESTIGATION OF THE OFFENCE

3. By section 63E of PoFA, the police are entitled to retain an arrestee's DNA profile and fingerprints until "*the conclusion of the investigation of the offence*" in which that person was suspected of being involved ("*or, where the investigation gives rise to proceedings against the person for the offence, until the conclusion of those proceedings*"). The Act contains no definition of that term.

4. In the absence of a definition of the term *"the conclusion of the investigation of the offence"* within PoFA, it was decided that the best (and only practical) course was:

   - to treat the moment at which an arrestee is 'No Further Action' (NFA) 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 Police National Computer as (in appropriate cases) the trigger for the automatic deletion of the arrestee's biometric records from the National DNA Database and IDENT1.

[237] 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.'

RETENTION AND DESTRUCTION REGIME

5. As regards DNA profiles and fingerprints 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.

6. In this context a 'recordable offence' is, broadly speaking, any offence which is punishable with imprisonment[238] 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.[239]

7. There are, however, a number of exceptions to that general rule, which are set out in detail below. The retention regime established by PoFA in respect of DNA profiles and fingerprints taken under PACE can be summarised in schematic form as set out in Table 11 at paragraph 40 of the main Report above.

INDIVIDUALS ARRESTED FOR QUALIFYING OFFENCES

8. A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.[240]

9. 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.

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

[238] See section 118 of PACE

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

[240] See section 65A(2) of PACE

INDIVIDUALS UNDER THE AGE OF 18 YEARS

10. PoFA introduced a more restrictive regime as regards the retention and use of biometric material taken from young people under the age of 18 years.[241]

- If a young person under the age of 18 years is convicted of a qualifying offence, their fingerprints and/or DNA profile may be retained indefinitely.
- If a young person is convicted of a minor recordable offence and receives a custodial sentence of more than 5 years, their fingerprints and/or DNA profile may be retained indefinitely.
- If a young person is convicted of a minor recordable offence but receives a custodial sentence of less than 5 years, their fingerprints and/or DNA profile may be retained for the duration of the custodial sentence plus 5 years. This is called an 'excluded offence'.
- If a young person is convicted of a second recordable offence, their fingerprints and/or DNA profile may be retained indefinitely.

PENALTY NOTICE FOR DISORDER

11. Where a penalty Notice for Disorder (a PND) is issued, biometrics may be retained for a period of 2 years.

MATERIAL RETAINED FOR THE PURPOSES OF NATIONAL SECURITY

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.[242] In such cases biometric material may be held on the basis of an NSD for a 2-year period. NSDs may be renewed before the date of their expiry for as many times as is deemed necessary and proportionate (see further **Appendix C)**.

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

13. Where a person without previous convictions is charged with a qualifying offence or where the Biometrics Commissioner accedes to an application under section 63G(2) or (3), by section 63F of PACE[243], the resulting 3 year retention 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. The decision of the District Judge may be appealed to the Crown Court.

[241] See section 63K of PACE (as inserted by section 7 of PoFA)

[242] See sections 63M and 63U of PACE as inserted by sections 9 and 17 of PoFA) and Schedule 1 of PoFA.

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

CONVICTIONS OUTSIDE ENGLAND AND WALES

14. By section 70 of the Crime and Policing Act 2017, which amends sections 63F, 63H, 63I, 63J, 63K and 63N of PACE, Police may retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample of persons convicted of a recordable offence under the law of a country or territory outside England and Wales where that offence is equivalent to a recordable offence in England and Wales. It should be noted that UK convictions under the laws of Scotland and Northern Ireland are treated as 'foreign convictions' for the purposes of biometric retention. This will only apply to biometrics taken in England and Wales on or after 03 April 2017[244].

15. For those persons whose biometrics were taken by police before 03 April 2017, by sections 61(6D), 62(2A) and 63(3E) of PACE[245] the police have, with the authority of an officer of the rank of inspector or above, power to take fingerprints and a DNA sample from any person who has been convicted outside England and Wales of an offence that would constitute a qualifying offence under the law of England and Wales. By section 63J of PACE[246] the police have the power to retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample. Although section 63J allows the police to retain for an indefinite period biometric material which has been taken under sections 61(6D), 62(2A) or 63(3E), it has no application to biometric material that has been or is taken under any other section of PACE. Biometric material which has been or is taken under any other such section (e.g. when an individual is arrested on suspicion of having committed an offence) cannot lawfully be retained indefinitely simply because the individual in question has been convicted of a qualifying offence outside England and Wales. If the police wish to retain the biometric records of such individuals and have no other basis for doing so, they have no option but to go back to those individuals and to take further samples and fingerprints from them under those sections.

[244] See also paragraphs 79 to 80 of the main Report above.

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

[246] (inserted by section 6 PoFA)

APPENDIX B

APPLICATIONS TO THE BIOMETRICS COMMISSIONER UNDER SECTION 63G PACE

THE RELEVANT STATUTORY PROVISIONS

1. 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.*
>
> *(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.*

2. 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.[247] Whereas a chief officer may only make an application under section

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

63G(3) if they consider that the retention of the material "*is necessary to assist in the prevention or detection of crime"*, section 63G(2) imposes no express requirement that there be some anticipated public interest in the retention of the material.

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

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

v. Although it is provided at sections 63G(5) and (6) that the person to whom the material relates must be informed of any application for extended retention and given the opportunity to make representations against it[248], 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.

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

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

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

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

CORE PRINCIPLES AND RELEVANT FACTORS

5. The approach which I decided to adopt to applications under section 63G(2) and (3) is set out in a document issued by my Office entitled *Principles for Assessing Applications for Biometric Retention.* The full document can be found at

https://www.gov.uk/government/publications/principles-for-assessing-applications-for-biometric-retention and its key provisions are as follows.

"Core Principles

1. The Commissioner will grant an application under section 63G(2) or (3) only if he is persuaded that the applying officer has reasonable grounds for believing that the criteria set out in those subsections are satisfied. Equally, however, he will not grant such an application merely because he is so persuaded. He will treat compliance with those criteria as a necessary, but not as a sufficient, condition for any conclusion that it is "appropriate" to retain the material at issue.

2. The Commissioner will grant such an application – and will consider the extended retention of such material 'appropriate' – only if he is persuaded that in the circumstances of the particular case which gives rise to that application:

- *there are compelling reasons to believe that the retention of the material at issue may assist in the prevention or detection of crime and would be proportionate; and*
- *the reasons for so believing are more compelling than those which could be put forward in respect of most individuals without previous convictions who are arrested for, but not charged with, a 'qualifying' offence.*

3. This will be the case for applications under both section 63G(2) and section 63G(3). The Commissioner will, however, be particularly alert to the possibility that extended retention may be appropriate in cases in which the criteria set out in Section 63G(2) are satisfied.

4. The Commissioner will require that the arrestee be informed – at least in general terms – of the reasons for any application and of the information upon which it is based. If the arrestee is not so informed of any reasons or information which the applying officer seeks to rely upon, the Commissioner will attach no weight to them.

Relevant Factors

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

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

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

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

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

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

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

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

OBC DOCUMENTS

6. In addition to the *'Principles'* document, The Office of the Biometrics Commissioner has published a number of other documents for use by the police and by the public in connection with applications under section 63G. These are available at https://www.gov.uk/government/organisations/biometrics-commissioner.

STRATEGY BOARD GUIDANCE

7. The Protection of Freedoms Act specifies that the National DNA Database Strategy Board may issue guidance about the circumstances in which applications may be made to the Biometrics Commissioner under section 63G, and that before issuing any such guidance that Board must consult the Commissioner.[249] The Strategy Board endorsed the approach which I had decided to adopt as regards such applications and the detailed Guidance document which it issued in September 2013 (and into which I had significant input) is consistent with the *'Principles'* and other documents that have been issued by my Office. A copy of the Strategy Board Guidance can be found at https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace.

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

8. If the Biometrics Commissioner accedes to an application under section 63G(2) or (3), by section 63F of PACE[250], the 3 year retention 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. The decision of the District Judge may be appealed to the Crown Court.[251]

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

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

[251] See further Appendix A: Applications to District Judges (Magistrates Court)

APPENDIX C

NATIONAL SECURITY PROVISIONS

STATUTORY BACKGROUND AND GUIDANCE AS TO NSDS

STATUTORY BACKGROUND

1. 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').

2. 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.

3. 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. The police and other law enforcement authorities may retain DNA profiles and fingerprints for an extended period on national security grounds but they may only do so pursuant to a National Security Determination or 'NSD'.[252]

4. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[253] 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,[254] in practice the same 2-year maximum is applied. An NSD may be renewed before its expiry for a further period of 2 years.

---

[252] 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.

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

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

5. 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.

6. 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.

7. The NSD process is primarily one for Chief Officers.[255] 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.

8. 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.

9. 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

[255] (see footnote 253 above).

Commissioner may order the destruction of the material if it is not otherwise capable of being lawfully retained.

STATUTORY GUIDANCE

10. 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.

11. A copy of the Guidance as issued can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf.
It would appear that the section dealing with DNA samples requires updating to take account of changes introduced by section 146 of the Anti-social Behaviour, Crime and Policing Act 2014.

NSD PROCESS

APPLICATIONS FOR NSDS

12. Applications for NSDs are compiled and submitted to Chief Officers by the Joint Forces Intelligence Team (JFIT) run by the MPS or, in Northern Ireland, by PSNI. 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."* [256]

13. 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

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

> *"45. The Chief Officer or Constable must carefully consider all relevant evidence in order to assess whether there are reasonable grounds for believing that retention is necessary for the*

[256] 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."*

purpose of national security. In doing so, they may wish to consider any or all of the following non-exhaustive categories of information:

a) Police intelligence

b) Arrest history

c) Information provided by others concerned in the safeguarding of national security

d) International intelligence

e) Any other information considered relevant by the responsible Chief Officer or Chief Constable.

46. The responsible Chief Officer or Chief Constable should also take into account factors including but not limited to the nature and scale of the threat to national security if the material is not retained and the potential benefit that would derive from the extended retention of the biometric material in question."

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

16. It is also expected, however, that Chief Officers will want to see more than a simple catalogue of historic facts and information about the individual and his or her associates. They will also want to be provided with a forward-looking analysis as to the nature of, and grounds for, existing and future concerns about the individual in question and with an explanation as to why it is believed that some genuinely useful purpose will be served by the retention of their DNA profile or fingerprints. The NSD process is, after all, primarily one which looks to the future rather than to the past.

NSD IT SYSTEM

17. 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. 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 the Commissioner's Office for review.

18. The NSD IT System does not allow the Commissioner's Office automatic access to all the underlying information and documentation that is referred to in an application for an NSD.

COMMISSIONER'S REVIEW PROCESS

19. When an application for an NSD is decided by a Chief Officer, the NSD IT System automatically informs the Commissioner's Office and forwards a copy of the case for review. 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 the Commissioner with documents and information, any requests for further information are, as a matter of practice, initially addressed to JFIT/PSNI.

20. Although the Commissioner's 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.*"

21. This is a striking power and it is clearly not one that the Commissioner can properly exercise merely because he/she is 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, the Commissioner is *neither* satisfied that an NSD has been properly made *nor* able to conclude that it is unnecessary for the material to be retained.[257]

22. In reality, then, the Commissioner has at least three options when reviewing an NSD:

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

    (ii) '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:

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

    but equally

[257] 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 the Commissioner feels able to conclude that it is not necessary for the relevant material to be retained, he/she is not persuaded that it would be right to order its destruction.

- the Commissioner 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) '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.

23. The NSD IT System provides for all three of those options. It also assumes that the Commissioner 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.

RETENTION AND USE OF BIOMETRIC MATERIAL FOR NATIONAL SECURITY PURPOSES

DNA SAMPLES

24. 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.

DNA PROFILES AND FINGERPRINTS

25. 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).

26. 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[258] 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. Parliament further agreed in October 2015 a one year extension of that transitional period until 31 October 2016[259]. In

[258] 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)

[259] 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)

practice, then, since 31 October 2013 Legacy Material which cannot otherwise lawfully be retained has been subject to a maximum retention period of 2 years unless an NSD is made in respect of it. If an NSD is made in relation to such Legacy Material before 31 October 2016, that material may be retained for the period that that NSD has effect.

27. For New Material, the retention period which applies in the absence of an NSD of course depends upon the legislation governing the powers under which it was taken. As regards material which has been taken under counter-terrorist legislation from individuals who have been arrested or detained without charge, the relevant retention periods in the absence of an NSD can be summarised in schematic form as follows:

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

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

CROSS-SEARCHING OF DATABASES

DNA PROFILES

28. The CT DNA Database is a standalone database of CT-related DNA profiles and crime scene stains. It is operated solely by the MPS's Secure Operations Forensic Services (SOFIS). 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.

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

FINGERPRINTS

30. Since 2012 all new ten-print fingerprint sets loaded to IDENT1 have been automatically washed through the CT Fingerprint Database.

APPENDIX D

Office of the Biometrics Commissioner, PO Box 72256, London, SW1P 9DU
Enquiries@BiometricsCommissioner.gsi.gov.uk

20 November 2017

Dear Chief Constable

I am writing to you in respect of the regime for the destruction of DNA samples for arrestees and volunteers under the Protection of Freedoms Act 2012 (PoFA). The general rule as regards the destruction of DNA samples is laid down in Section 63R(4) PACE (as amended by section 14 Protection of Freedoms Act 2012). That section states that:

> *(4) a DNA sample to which this section applies must be destroyed –*
>
> *(a) as soon as a DNA profile has been derived from the sample, or*
>
> *(b) if sooner, before the end of the period of 6 months beginning with the date on which the sample was taken.*

One notable exception to this rule was introduced by Section 146 of the Anti-social Behaviour Crime and Policing Act 2014 (amending Section 63U(5)of PACE), which states that where a sample *"is or may become disclosable under the Criminal Procedure and Investigations Act 1996, or a code of practice prepared under section 23 of that act or in operation by virtue of an order under section 25 of that Act",* the sample may be retained until it has fulfilled its intended use, or if the evidence may be challenged in court, until the conclusion of judicial proceedings and any subsequent appeal proceedings.

Section 146 continues *'A sample that once fell within subsection (5) but no longer does, and so becomes a sample to which section 63R applies, must be destroyed immediately if the time specified for its destruction under that section has already passed."*

It is clearly open to forced 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. It has come to the Biometrics Commissioner's attention, through visits to forces and discussions with key stakeholders that forces are interpreting and applying the CPIA exception inconsistently.

In the last 18 months, the Commissioner has seen a rapid rise in the number of samples – both PACE arrestee and volunteer/elimination – held under this exception both in force and with Forensic Service Providers. In addition reviews of DNA samples, which have been held with Forensic Service Providers for over 18 months, have shown that the vast majority of B scrape samples retained under the CPIA exception have not been used for further/specialist analysis. It appears therefore that, at least for some police forces in England and Wales, routine and/or 'blanket' retention of large numbers of DNA samples under CPIA has become the norm. As such very real questions have arisen as to whether Parliamentary intention that DNA samples be routinely destroyed is being circumvented. Consequently it could be argued that the lawfulness of the continued retention of many of the DNA samples at issue has been called into question.

In the absence of specific guidance on the use of this exceptional retention power, the Biometrics Commissioner has sought to set out key principles in respect of the operation of the CPIA exception, against which he will inspect going forward. It is envisaged that the new audit regime in respect of CPIA holdings (in force and with Forensic Service Providers) will commence from April 2018.

Key Principles

2. 1. ***It is the Biometrics Commissioner's position that retention under CPIA is an exception power; it should not be used as a blanket means of retention for certain types of offences or more generally.*** While it may be more likely that CPIA will be considered for serious crimes, this should be a start point for further interrogation of the case, not the end point in terms of a retention decision. All decisions for retention under CPIA should be taken on a case-by-case basis with specific reference to the circumstances of the particular offence under investigation. Retention under CPIA should only be requested where it is clear that further analysis is, or may be, required as part of the forensic strategy for the given investigation. It should be noted that the decision to retain must consider the appropriateness of the retention and data minimisation principle defined within CPIA.

3. 2. ***Centralised records should be kept of all samples retained under CPIA, both in force and with Forensic Service Providers.*** The following information should be recorded as a minimum:

- Barcode reference
- Location of retained sample
- Sample date
- Date of retention request
- Person authorising retention
- Review dates

- Reason/justification for retention
- Date of request for destruction

4. All methods of recording should be fully auditable against the above categories as a minimum.

5. 3. ***CPIA retention decisions must be evidenced.*** Forces must evidence the necessity of the retention. Retention decisions and the justification for those decisions should be made and recorded centrally. Retention decisions should be made by those familiar with the forensic/scientific strategy for the case and who are aware of the PoFA and CPIA retention rules. Decisions to retain samples under CPIA must be scrutinised at an appropriate level within organisations to avoid 'just in case' retentions.

6. 4. ***All DNA Samples retained under CPIA must be subject to quarterly review as a minimum.*** Forces receive quarterly reports form Forensic Service Providers as to the PACE arrestee and Elimination samples being held under CPIA. Those lists *must* be reviewed on receipt and appropriate action taken to ascertain whether those samples are still required to be retained. Ongoing retention decisions should be made by those familiar with the forensic/scientific strategy for the case and who are aware of the PoFA and CPIA retention rules. Decisions to retain samples under CPIA must be scrutinised at an appropriate level within organisations to avoid 'just in case' retentions.

7. An equivalent approach should be taken with DNA samples held in force, with all DNA samples (PACE arrestee and Elimination) subject to quarterly review.

8. As set out above, under the CPIA exception, a sample should only be retained for the purposes of further analysis or where *"it is, or may become, disclosable in court".* Therefore, it is the commissioner's view that if a DNA sample has never been used in casework where, from the facts of the case, it is clear that the sample has not been and will not be required in evidence, the DNA sample should be destroyed; this may well be before the investigation is concluded.

Forces should seek to avoid the situation whereby DNA samples are retained for extended periods despite those samples never having been used.

5. ***All DNA samples held under CPIA in force should be appropriately stored and monitored.*** Through visits to England and Wales forces, it has become clear that a number of forces are retaining a large number of PACE arrestee and Elimination DNA samples in force within detained property stores. In some instances these samples are not stored and reviewed with the same rigour afforded to DNA samples held with Forensic Service Providers.

Where DNA samples are held within force the following points should be considered:

- DNA samples should be kept separately from other evidential material. This would ensure that proper PoFA review can be undertaken and that samples are not overlooked whilst stored.

- There should be no difference between the decision-making processes, authorisation of retention, recording, treatment and review of DNA samples held in force and those samples held by Forensic Service Providers – see further Points 1 to 4 above.

If existing force property management systems do not adequately allow for the proper management of DNA samples under PoFA and CPIA – including recording of the reasons/ justification for retention of such samples – additional recording methods should be implemented as set out at Point 2. Any property management system holding data on CPIA retention should be fully auditable as set out at Point 2.

6. ***All in force holdings must be reported to the National DNA Database Delivery Unit (NDU) on a quarterly basis.***

Since October 2013, there has been a requirement to provide quarterly returns on the numbers of PACE arrestee and Elimination DNA samples held in force to the NDU. In turn, those figures are reported to the Biometrics Commissioner's Office. It is evident from those returns that many forces are not complying with this requirement. The first quarterly return for 2018 will be due in April 2018. From April 2018, any force which fails to provide a return to the NDU on its in force holdings will receive a notice of non-compliance from the Commissioner's Office and may be subject to further audit by the Commissioner's Office. ALL notices of non-compliance will be reported in the Commissioner's Annual Report.

Thank you in advance for your cooperation. Any queries regarding this letter or the requirements set out herein, should be forwarded to Enquiries@BiometricsCommissioner.gsi.gov.uk.

Yours sincerely

Gemma Gyles
Office of the Biometrics Commissioner
For and on behalf of the Biometrics Commissioner

LIST OF ACRONYMS

ABH	Actual Bodily Harm
ACPO	Association of Chief Police Officers (now known as the National Police Chiefs' Council ('NPCC')
ACRO	ACRO Criminal Records Office
BRU	Biometric Retention Unit
CODIS	Combined DNA Index System
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
FINDS	Forensic Information Databases Service
FINDS-DNA	Forensic Information Databases Service's DNA Unit
FINDS–SB	Forensic Information National Databases Strategy Board
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
NFA	No Further Action
NLEDS	National Law Enforcement Data Programme
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
UKAS	United Kingdom Accreditation Service
UKICB	United Kingdom International Crime Bureau

CCS0518559084
978-1-5286-0370-6