ANNUAL REPORT 2016

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Paul Wiles

March 2017

Office of the Biometrics Commissioner

ANNUAL REPORT 2016

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.

September 2017

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

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

ISBN 978-1-5286-0032-3

CCS0917991760 09/17

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 third 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 14th March 2017. I understand that the publication of the Report was then delayed by the convention limiting the publication of government related material until after the election. For similar reasons the publication of the previous Annual Report was delayed for three months. The effect of these two delays is that since the implementation of the Protection of Freedoms Act in 2013 the number of annual reports is now one less than it ought to have been.

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.

I had the good fortune to inherit a first class Office of the Biometrics Commissioner and without the help of the staff therein I would not have been able to complete this Annual Report so soon after my appointment.

Since my appointment is part-time the Head of my Office, Gemma Gyles, not only runs the Office on a day-to-day basis but acts on my behalf much of the time. Without her encyclopaedic knowledge of PoFA, and its operating details in practice, the job of the Commissioner would be very difficult. I want to record my thanks to her and my gratitude for her commitment to ensuring that the PoFA regime for biometric use and retention operates as Parliament intended. In the same way I want to record my thanks to Lucy Bradshaw-Murrow, Jim McAVeety and Aradhna Jaswal who have made the casework component of my role manageable. To all of them I am most grateful.

Paul Wiles

March 2017

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 (PoFA) 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. I am the second person to hold the position of Biometrics Commissioner and took up the role in June 2016 after an open public appointments process. This is the third Annual Report of the Biometrics Commissioner on the biometric aspects of PoFA.

3. The task of identifying and dealing with the initial problems of implementing PoFA fell to my predecessor, Alastair R MacGregor, QC. This was done with great legal expertise, thoroughness and skill and I am very grateful for the legacy left me. Very sadly Alastair was taken ill and died quite shortly after I came into post and I miss his wise counsel. He was devoted to ensuring that public interest and individual rights were properly balanced as intended by PoFA and he was a model of legal professionalism, public service and commitment.

1.2 THE PASSING OF THE PROTECTION OF FREEDOMS ACT 2012

4. Prior to 2012 the legal position in England and Wales was that DNA samples, DNA profiles and fingerprints ('biometrics') could be kept indefinitely for anyone arrested for a recordable offence, which are largely all but the most minor offences.[2] In 2008 the Grand Chamber of the European Court of Human Rights (ECtHR) in *S and Marper v United Kingdom*[3] held that this position was not lawful because the indiscriminate retention regime in operation in England, Wales and Northern Ireland was disproportionate. The Labour

---

[1] See further Section 5 of this Report.

[2] A recordable offence is an offence which must be recorded for the Annual Crime Statistics. Generally, an offence that could result in imprisonment is classed as a recordable offence (i.e. an indictable or triable-either-way offence). There are also some more minor summary offences that are designated as recordable as laid out in The National Police Records (Recordable Offences).

Regulations 2000 (http://www.legislation.gov.uk/uksi/2000/1139/pdfs/uksi_20001139_en.pdf)

[3] (2008) 48 EHRR 1169

government of the day passed the Crime and Security Act 2010, which laid down a new retention regime, but the relevant provisions were not commenced before the 2010 General Election. The incoming coalition government considered that the provisions in the Crime and Security Act were inadequate so brought forward PoFA in 2012, which repealed the relevant parts of the previous legislation and introduced a different regime. The general change brought about by PoFA was that biometrics can now only be kept indefinitely for individuals convicted of a recordable offence, and shorter retention periods apply to those charged but not convicted of serious offences, for young people and on grounds of national security. In addition, the police can apply to the Commissioner to retain for three years the biometrics of those arrested but not charged of certain more serious offences.

5. This new regime is more proportionate but, as a result, significantly more complicated than the previous position.

1.3 USE OF BIOMETRICS BY THE POLICE

6. DNA is an effective way of identifying an individual or, if biometric material is found at a crime scene or on a victim, the person to whom the material relates. This is based on extensive and good scientific evidence which provides the basis for analytic techniques that give high probabilities that claimed matches are true. Fingerprints are based on less extensive scientific evidence but can provide a number of possible matches which are finally decided on the basis of judgments by trained staff. The scientific basis for using these types of biometrics in criminal investigations is therefore good.[4]

7. Furthermore, the quality of such techniques is overseen by the Forensic Science Regulator, Dr Gillian Tully, as is the way in which evidential claims are made.[5] 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.

1.4 PRESENTING BIOMETRIC EVIDENCE

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

---

[4] For a fuller account of the police use of DNA see: *National DNA Strategy Board, Annual Report 2015/16 (*http://www.gov.uk/government/publications/national-dna-database-annual-report-2015-to-2016*)*.

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

9. How well those involved in the criminal justice process, from police investigators to juries, understand such scientific judgments has not been fully examined. Whether the manner in which such evidence is presented would change the understanding of it is also not fully understood, yet is capable of empirical investigation.

10. This is one of a number of areas where my remit overlaps with that of the Forensic Science Regulator and we have discussed how we can work together in such areas in the future. In this case we intend to work with the Royal Statistical Society (RSS), and others with expertise and experience of criminal justice decision making, to develop and test a standard means of presenting the quality and strength of forensic evidence to help those involved in criminal justice decision making. We are grateful to Professor Sir David Spiegelhalter, the President of the RSS, for his support in this matter.

2. BIOMETRIC DATABASES

2.1 THE GOVERNANCE OF THE NATIONAL DNA & FINGERPRINT DATABASES

11. The National DNA Database (NDNAD) is overseen by the National DNA Strategy Board (NDNASB), which was given a statutory role in PoFA.[6] It is chaired by a representative of the National Police Chiefs' Council and includes representatives of the Home Office, the Chair of the National DNA Database Ethics Group,[7] the Forensic Science Regulator, the Biometrics Commissioner, the Information Commissioner[8] and representatives of the devolved administrations. The Strategy Board monitors the performance of the database and its use by the police and publishes an Annual Report.[9] It also issues guidance on the police collection and use of DNA, including meeting the requirements of PoFA.

12. Until recently the national fingerprint database (IDENT 1) did not have a similar governance structure, although limited progress in this regard had been made through the Fingerprint Governance Board and its operational police-led working group, the Fingerprint Strategic Network. My predecessor commented unfavourably on this lack of adequate governance in his 2015 Annual Report.[10]

13. Since March 2016, however, fingerprints have been added to the remit of the Strategy Board and it has become the National DNA Database & Fingerprint Database Strategy Board (NDNAD&FSB). This is a welcome development since it brings fingerprints within a proper, transparent and, moreover, mature national governance structure. There are, however, other police biometric databases that are not within the remit of the NDNAD&FSB, most notably the facial images held on the Police National Database (PND), of which more later.

14. DNA, from the beginning of its use by the police, has had a national database and a central management and governance framework. The police use of fingerprints, being much older, is still a much more dispersed system with the vast majority, but not all, fingerprints being on the national fingerprint database (IDENT1) and some separate holdings of hardcopy prints at force level and within the National Fingerprint Archive. One of the challenges for the new NDNAD&FSB will be to bring the collection, use and governance of fingerprints to the same standard as that of DNA.

---

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

[7] See http://www.gov.uk/government/organisations/national-dna-database-ethics-group

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

[9] (www.gov.uk/government/publications/national-dna-database-annual-report-2014-to-2015)

[10] *Commissioner for the Retention & Use of Biometrics, Annual Report 2015*, at paragraphs 326-328.

2.2 DATABASE HOLDINGS

NATIONAL DNA DATABASE

15. The National DNA Database was established in 1995 and, by the end of the calendar year 2016, held 5,462,627 subject DNA profiles for England and Wales. This equates to an estimated 4,784,954 individuals. UK holdings total 6,530,647 subject and crime scene profiles or an estimated 5,231,849 individuals out of a population of 65,110,000 (8%).[11] 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 246,400 in 2015/2016.[12] The number of crime scene profiles added to the database has also declined but by no means to the same extent and probably reflects changing priorities as regards the deployment of police resources rather than the number of offences reported/investigated.[13] Additional Data on NDNAD holdings can be found at **Appendix A**.

TABLE 01: Number of DNA profiles held by the end of December 2016

	Subject profiles	Crime Scene profiles	Total
England & Wales[14]	5,462,627	521,683	5,984,310
Rest of UK[15]	521,462	24,875	546,337
Total	**5,984,089**	**546,558**	**6,530,647**

(Source: National DNA Database Delivery Unit[16])

[11] ONS: Population Estimates for UK, England and Wales, Scotland and Northern Ireland: Mid-2015, June 2016. The percentage is actually higher because the denominator ought to exclude those below the age of criminal responsibility.

[12] *National DNA Strategy Board, Annual Report 2015/16*, figure 2a.

[13] From 44,000 in 2009/10 to 36,300 in 2015/16 (*National DNA Strategy Board, Annual Report 2015/16,* figure 2b).

[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 the National DNA Database Delivery Unit for their help in preparing the relevant data.

TABLE 02: Total DNA Holdings on NDNAD by Profile Type (year ending 31 December 2016)

	Arrestee	Volunteer[17]	Crime-scene from mixtures[18]	Crime-scene non-mixtures	Unmatched Crime-scenes[19]
England & Wales	5,462,627	2,010	54,373	467,310	173,922
Rest of UK	521,462	2,165	1,056	23,819	16,017
Total	**5,984,089**	**4,175**	**55,429**	**491,129**	**189,939**

(Source: National DNA Database Delivery Unit)

NATIONAL FINGERPRINT DATABASE: IDENT1

16. The National Automated Fingerprints Identification System (NAFIS) became operational in 1998 for ten-prints and fully operational in 2001. Livescan[20] came into operation with NAFIS in 2002. NAFIS was succeeded by IDENT1 in 2004.

TABLE 03: Number of fingerprints held on IDENT 1 for all forces as at 30 September 2016

Arrest Records	Subject Ten-Print Fingerprints[21]	Unmatched Crime Scene Finger-marks	Unmatched Palm Marks
23,836,130	7,962,091	1,977,796	354,925

(Source: National DNA Database and Fingerprint Database Strategy Board)

[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 a system for capturing fingerprint and palm data on an electronic scanner and then comparing that data with that already held on the national fingerprint database, IDENT1.

[21] Taken under PACE or equivalent.

TABLE 04: Total Holdings on IDENT1 by classification (30 September 2016)

Arrest Records	Subject ten-print fingerprints[22]	Pseudo Sets[23]	Unmatched Crime Scene Finger-marks	Unmatched palm marks	No of Cases with Unidentified Crime marks	Cases in Serious Crime Cache
23,836,130	7,962,091	4,710	1,977,796	354,925	1,010,747	1,113

(Source: National DNA Database and Fingerprint Database Strategy Board)

2.3 THE USE OF THE DATABASES AND ATTRITION RATES

NATIONAL DNA DATABASE

ADDITIONS TO THE NDNAD IN 2016

17. The National DNA Database as of the year ending 31 December 2016, held 5,984,089 subject profile records and 546,558 crime scene profile records. In 2016, 531,592 new subject profiles were added to the database, and 40,084 crime scene profiles were also added to the database (See Table 05 below).

TABLE 05: Additions to the NDNAD (January-December 2016)

	Arrestee	Volunteer[24]	Crime-scene from mixtures[25]	Crime-scene non-mixtures
England & Wales	251,927	4	23,810	14,766
Rest of UK	279,665	18	378	1,130
Total	531,592	24	24,188	15,896

(Source: National DNA Database Delivery Unit)

18. The National DNA Database Strategy Board Report shows that the number of subject profiles held on the database reached a peak of 6.97 million in the fiscal year 2011/12, declined to 5.63 million in 2012/13 and then increased to its present level of 5.86 million:

[22] Taken under PACE or equivalent.

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

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

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

this is because the number of new profiles loaded has declined from 54,000 in the fiscal year 2009/10 to 29,200 in 2015/16. The number of crime scene profiles loaded onto the database has declined from 50,000 in 2008/09 to 39,000 in the fiscal year 2015/16.

19. In 2015/16, 205,977 subject profile records were deleted from the database and 4,547 crime scene profile records were deleted.[26]

MATCH RATES

20. The extent to which crime scenes are examined for DNA stains varies significantly between offence types.[27] 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.

21. Given that most of those convicted of a recordable offence will have their DNA and fingerprints retained,[28] 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 67.5% for England and Wales) and is slowly increasing as profiles of more known offenders are added to the database.[29]

TABLE 06: Match Rate for Matches obtained immediately on loading for England and Wales Forces (year ending 31 December 2016)[30]

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	**38,576**	**251,927**
No. of Matches	26,045 (67.5%)	4,784 (1.9%)

(Source: National DNA Database Delivery Unit)

[26] Comparative figures on deletions are not available for the calendar year ending 31 December 2016.

[27] See *National DNA Database Strategy Board Annual Report 2015/16* , Table 1, page 9.

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

[29] See *National DNA Database Strategy Board Annual Report 2015/16*, Figure 4, page 14.

[30] 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.

TABLE 07: Match Rate for Matches obtained immediately on loading for all UK forces (year ending 31 December 2016)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	**40,084**	**279,665**
No. of Matches	26,509 (66.1%)	5,272 (1.9%)

(Source: National DNA Database Delivery Unit)

22. Table 08 below shows the match rates for crime scene profiles loaded to the NDNAD by England and Wales forces where those crime scenes have matched against subject profiles loaded to the database by Police Scotland and Police Service Northern Ireland. Similarly the second table shows match rates for crime scene profiles loaded to the NDNAD by Police Scotland and PSNI where those crime scenes have matched against subject profiles loaded to the NDNAD by England and Wales forces.

TABLE 08: Matches to Scottish and Northern Irish DNA Profiles (January-December 2016)

No. of crime scene profiles loaded by England & Wales	**38,576**
No. of crime scene profiles which have matched a subject profile loaded by Police Scotland.	166 (0.4%)
No. of these matches where the Scottish subject was the only subject to match the crime scene.	21 (13%)
No. of crime scene profiles which have matched a subject profile loaded by Police Service Northern Ireland	29 (0.08%)
No. of these matches where the Northern Ireland subject was the only subject to match the crime scene.	5 (17%)

	Police Scotland	Police Service Northern Ireland
No. of crime scene profiles loaded by force	**879**	**461**
No. of these crime scene profiles loaded which have matched a subject profile loaded by England and Wales forces.	41 (4.6%)	21 (4.6%)
No. of these matches where the English/Welsh subject was the only subject to match the crime scene.	34 (3.9%)	11 (2.4%)

(Source: National DNA Database Delivery Unit)

23. Table 08 suggests that there is a relatively low rate of cross-border crime within the UK. This might be explained by findings in Home Office research which has shown that generally offenders do not travel far.[31]

24. Police Scotland and Police Service Northern Ireland gain somewhat more intelligence about crime elsewhere in the UK by putting their data on the NDNAD than do England and Wales forces.

ATTRITION RATES

25. Whilst match rates might be high, the proportion of all crimes for which DNA is involved in an outcome for that crime is low.[32] The attrition rate from a crime being recorded by the police to a match being found to a DNA subject profile present on the NDNAD can be seen in Table 09. This shows the attrition rate for all recorded crime in England and Wales and for those crimes for which DNA is most commonly collected from crime scenes. DNA plays an important role in contemporary policing yet in only 0.3% of recorded crime was DNA involved in the resulting case outcome.[33]

26. As can be seen DNA is not involved in the police achieving an outcome in the vast majority of crimes reported to the police[34], although it is much more important for some of the more serious crimes. The House of Commons Science & Technology Committee and the Government Chief Scientific Advisor have made a similar point about forensics in general.[35]

---

[31] Wiles, P. and Costello, A. (2000). *The 'Road to Nowhere': The Evidence for Travelling Criminals*. Home Office Research Study 207. Home Office; London. And see also: Hodgkinson, S and Tilley,N (2007): *Travel-to-Crime: Homing in on the Victim*, International Review of Victimology, Vol 14, 281-298.

[32] A new 'Recorded Crimes Outcomes Framework' was introduced in April 2014 which allows every crime recorded by the police to be given a detailed outcome, not all of which are convictions. See: https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2015-to-2016

[33] (See footnote 32)

[34] The rate would, of course, be even lower if total crime as estimated by the Crime Survey of England and Wales was used as the denominator. For these purposes, 'crimes recorded by the police' is an appropriate denominator to measure the crime demand known to the police.

[35] See House of Commons Science & Technology Committee*: Forensic Science Strategy*, *Fourth Report of Session 2016-17*, at paragraph 3.5; and Government Office for Science, *Annual Report of the Government Chief Scientific Advisor 2015, Forensic Science and Beyond: Authenticity, provenance and Assurance*, 2015, page 6.

TABLE 09: Attrition rate from recorded crime to outcome involving DNA

	All Crimes	Theft of Vehicles	Domestic Burglaries	Rapes	Homicides
Total police recorded crime	**3,775,365**	**80,058**	**189,951**	**34,402**	**1,265**
Crime scenes examined	11% (416,715)	28.7% (23,009)	80.3% (152,444)	19.8% (6,818)	96.9% (1,226)
No. which yielded DNA	2.4% (89,149)	11.3% (9,084)	13.3% (25,210)	7.8% (2,679)	63.5% (803)
No. DNA submitted for analysis	1.8% (68,055)	8.1% (6,519)	10.1% (19,368)	6.4% (2,201)	38.7% (490)
No. loaded onto database	0.5% (22,584)	2.3% (1,862)	3.4% (6,438)	1.1% (387)	10.4% (132)
No. linked to outcome	0.3% (11,378)	0.9% (759)	1.4% (2,589)	0.6% (215)	8.4% (108)

ERROR RATES

27. Whilst error rates[36] that are found in the processing of DNA are generally acceptable, those currently found when subjects' DNA samples are taken appear to be unacceptably high and vary by force. The NDNADSB has identified this problem as in need of urgent investigation and improvement.[37]

28. Since April 2016, the NDU has collected data on errors in DNA sampling by police forces, both at crime-scenes and in custody. This data is provided to the NDU by the relevant police forces. The data collected has not yet been fully verified and therefore further work is required before conclusions can be drawn. However, only a limited number of forces have responded to requests for data. This is worrying since one would expect forces that have adequate governance processes to be able to provide such data.

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

[37] *National DNA Database Strategy Board Annual Report, 2015/16*, Table 5: Error Rates, at page 26.

29. The NDU also produces data on the number of confirmed errors discovered on the NDNAD. Although errors were identified in the period January to December 2016, the relevant profiles could have been loaded to the NDNAD at any point in the previous 2 years. 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. Again further verification work is required before sound conclusions can be drawn.

NATIONAL FINGERPRINT DATABASE: IDENT1

ADDITIONS TO IDENT1 IN 2016

30. IDENT1 as at 30 September 2016, held 7,962,091 unique arrestee subject ten-print records, 1,977,796 unmatched finger-marks and 354,925 unmatched palm prints relating to 1,010,747 cases with unidentified scenes of crime marks. In the quarter ending 30 September 2016, 24,987 unique subject records and 4,029 crime scene cases were added to the database (See Table 10 below).[38]

TABLE 10: Additions to the Database for England & Wales (July-September 2016)[39]

Arrest Records	Subject Ten-print Fingerprints	Crime Scene Marks[40]	Serious Crime Cache[41]
24,987[42]	246,424[43]	4,029	2

(Source: National DNA Database and Fingerprint Database Strategy Board)

31. In the quarter ending 30 September 2016, 1,732 PACE subject records were deleted from the database.[44]

[38] The quoted figures represent the net increase in records held on IDENT1 accounting for the overall difference of records added and deleted from June to September 2016.

[39] The current format and reporting of IDENT data to the NDNAD&FSB equivalent to that available for the NDNAD has only been in place since July 2016, hence limited statistics are available in respect of finger and palm prints.

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

[41] (see footnote 40 above)

[42] Figure provided refers to the number of unique PACE subject records added to IDENT 1.

[43] Figure provided refers to the total number of arrests processed. The number of unique records added to IDENT1 is 24,987.

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

MATCH RATES

32. The match rate for fingerprints and palm prints, compared to that for DNA is currently difficult to calculate since the data available to us is basically contract compliance data and not designed for this purpose. In theory one might expect match rates to be similar to those for DNA since fingerprints are routinely taken at arrest and similarly searched for at crime scenes. Now that fingerprints have been added to the remit of the NDNAD&FSB we can expect to see this data in its next annual report.

33. 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]

2.4 KNOWLEDGE BASE ON BIOMETRIC USE EFFECTIVENESS

34. It does not follow that where crimes are detected or 'solved' by the police, all those detections where biometrics were available occurred because of a biometric match: the offender may have been identified for other reasons and the biometric holdings may have played no role or were merely confirmatory. Given the attrition rates cited above and the difficulty of attributing crime outcomes to biometrics, there are currently unanswered questions as to the cost-effectiveness of police use of biometrics.[46]

35. The College of Policing was set up in 2012 as a national professional body for the police service and one of its key functions is to provide a knowledge base to enable the police to take evidence-based decisions.[47] Nevertheless, the fact that the science behind DNA and

---

[45] DNA samples are usually taken in custody in relation to major crimes or where an existing DNA profile has been obtained using SGM or SGMplus 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.

[46] The same point was made in the *Forensic Science Strategy*, Cm 9217, at paragraphs 45-46; *Forensic Science Regulator Annual Report 2016* (FST004), at paragraph 8; and by the *House of Commons Science & Technology Committee, Fourth Report of Session 2016-17*, at paragraph 35.

[47] See www.college.police.uk

fingerprints is well known and their use well regulated does not necessarily mean that the collection and use of biometrics in the criminal justice system produces benefits that otherwise would not happen, nor that their use is cost-effective. The difference between theoretical and actual benefits in a particular situation is yet to be determined.

36. In respect of the retention and use of biometrics in England and Wales well-designed systematic research has yet to be carried out on this system benefit question. Some research has been carried out in the USA[48] but the use of biometrics in the two countries is sufficiently different to mean that the results cannot be straightforwardly carried across. The American evidence points to the fact that DNA is particularly important in bringing more serious offenders to justice and the same may well be true in the UK; however, without well designed empirical research, this frequently stated hypothesis cannot be tested or proven.

37. This lack of a good evidence base does not mean that the retention and use of biometrics is not important or effective in the criminal justice system; indeed all observation suggests that it is. What is not clear is what the investment return is on a particular biometric as compared to investing in other policing procedures. As the range and complexity of biometrics used by the police increases (see Section 8 of this Report below) it will be important to have such a knowledge base for all biometric types so that the police can determine the optimum mix of biometrics for different crime types in order to best employ scarce resources. At present the College of Policing cannot provide such empirical knowledge and does not have an established research programme to do so in the future. The police service is aware that, as new biometrics are deployed, it will need such knowledge to judge future investment decisions and, as part of its response to the new Forensic Science Strategy[49], it is seeking ways to fill this knowledge gap.

---

[48]Roman, JK et al: *The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes*, Urban Institute, Justice Policy Center, 2008.

[49]http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/506652/54493_Cm_9217_Forensic_Science_Strategy_Accessible.pdf

3. BIOMETRIC RETENTION & POFA COMPLIANCE

3.1 THE BIOMETRIC REGIME INTRODUCED BY POFA

38. 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 those 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

39. 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.

40. Although the police have taken 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).

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

42. DNA profiles derived from DNA samples taken from an arrestee are loaded onto the National DNA Database (NDNAD).

SUMMARY OF POFA RETENTION RULES

43. 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 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;[50]
- that if an individual is convicted of a recordable offence the 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'[51]) then the 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 B** 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**

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

[51] 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[52] 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)**

THE MEANING OF 'INDEFINITE' RETENTION

44. There has been some debate and disagreement as to what 'indefinite' biometric retention means in practice.

45. The plain meaning would be that the biometrics may be retained forever. Whilst this is a simple concept to employ, over time 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.

46. Existing National Police Chiefs' Council (NPCC) Guidance on the Deletion of Records from National Police Systems[53] sets out that, regardless of outcome, police records should be retained until a subject is deemed to have reached 100 years of age. The interpretation of 'indefinite' as being the date at which a person is deemed to have reached 100 years of age seems to me a practical and workable solution that will prevent the databases holding material of no further policing value. Even then, records could be retained if there is still an

---

[52] 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.

[53] http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430095/Record_Deletion_Process.pdf

open investigation involving the subject. This is the solution adopted in Scotland. I understand that this issue has been referred to the National DNA Database Ethics Group for discussion and comment. I shall continue to monitor this issue and press for a speedy conclusion.

FOOTWEAR IMPRESSIONS

47. Footwear impressions are not a biometric but nevertheless they are included in PoFA. Section 63S of PoFA 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."*[54]

48. It is not clear to me at present how these retention rules are applied by police forces. I have therefore written to Chief Officers asking for a copy of their policy as regards the retention of footwear impressions and will report on this in due course.

49. Where relevant, most forces take footwear impressions both from suspects and at crime scenes and new technology for doing so is coming into use. Indeed, the Metropolitan Police have been trialling the routine collection of footwear impressions as people enter custody suites.

50. There are 2 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 the National DNA Database Delivery Unit (NDU).

51. I have been advised that 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.

52. Because footwear impressions are not a biometric, their utility is short-lived since shoes will wear over time and the impressions they leave will inevitably change. Therefore, I was puzzled to learn that impressions are not deleted from either the NFRC or the NFD, but are held indefinitely for reference purposes. Only duplicates are deleted if a request is made by the relevant police force. This is an area which I will be examining in the coming months.

---

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

3.2 PROVIDING ASSURANCE ON POFA COMPLIANCE

53. 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. This report is about compliance with the PoFA regulation of the use and retention of fingerprints and DNA.

54. The three independent Forensic Service Providers (FSPs)[55] 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 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 formalized in the context of the current UKAS assessment mechanism, and it is envisaged that such checks will be conducted during assessment visits by UKAS every other year.

55. As far as police forces are concerned, the previous Commissioner's assurance was based on a number of inspection visits, some limited data collection and experience of the caseworking functions of the Commissioner. This approach identified a range of compliance issues, many of which were reported in the first and second Annual Reports and are still waiting to be resolved or are now in the process of being resolved.[56]

56. The limited resourcing of the Commissioner's Office meant that it was not possible to visit all England and Wales police forces each year and so annual assurance was always going to be partial. To date, this has not been a problem, since the early compliance issues were rarely unique to one force, but it has led me to re-think how compliance should be monitored annually, particularly since the limitation of resourcing is not likely to change in the near future.

57. In future, 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.[57] In

---

[55] LGC Ltd, Orchid Cellmark Ltd and Key Forensic Services Ltd.

[56] (see paragraphs 62-85 of this Report below)

[57] I am grateful to Kirsty Faulkner, Head of the NDNAD National Delivery Unit for her help in this regard.

addition, the new governance structure for fingerprints should ensure that management information for fingerprints is more accessible, open and transparent. Descriptive analysis of such data will provide an annual national picture of compliance and how this varies by force or biometric type and use. The present report contains a little more of this descriptive data but the intention is to expand this, where possible, in the future.

58. It may also be possible to carry out some explanatory analysis of the data to understand the reasons for the descriptive picture. It is envisaged that this annual descriptive analysis will inform a programme of force inspection visits on a risk basis, which can be combined with casework information, to provide an overall assurance picture.

59. Police forces will also need to monitor their PoFA compliance by having and implementing 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. The present report begins the transition to this new approach.

3.3 ASSURANCE IN NORTHERN IRELAND

60. My predecessor reported last year that he had been approached by both the Police Service of Northern Ireland (PSNI) and the Department of Justice (Northern Ireland) to ask if he would provide non-statutory oversight of the PACE retention regime in Northern Ireland.[58] This was because although the Northern Ireland Assembly had passed legislation that would have allowed them to appoint their own 'Northern Ireland Commissioner for the Retention of Biometric Material' it has not yet been possible to secure cross party support to enable commencement of the provisions which the Northern Ireland Commissioner for the Retention of Biometric Material was envisaged to oversee.[59] In the event it was decided to leave this matter until the new Biometrics Commissioner for England and Wales was appointed.

61. I informed the Department of Justice (Northern Ireland) that I did not think it proper to provide oversight on a non-statutory basis and, on this basis, it has been agreed that this matter will not be pursued at this time. PSNI have taken steps to make their process nearer to PoFA whilst they await the commencement of the Northern Irish legislation. Until the Northern Ireland Executive implements their legislation they will not have fully responded

[58] See *Commissioner for the Retention and Use of Biometrics, Annual Report 2015*, at Paragraph 333.

[59] See Criminal Justice (Northern Ireland) Act 2013

to the judgment of the ECtHR in *S & Marper v UK*;[60] however, since this is a devolved matter, it is an issue for the Northern Ireland Executive.

3.4 POFA COMPLIANCE: ISSUES IDENTIFIED IN PREVIOUS ANNUAL REPORTS

62. The previous Commissioner reported that the police were largely compliant with the requirements of PoFA, whilst drawing attention to a number of areas that needed clarification by way of further guidance. I have seen nothing that casts doubt on this overall judgment and it is clear that the police have worked hard to ensure that their processes follow the requirements of the legislation.

63. Notwithstanding this overall assessment, and as the previous Commissioner reported, 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 some have remained as was reported in the last two Annual Reports.[61] This was still the case when I came into post even though some of these issues had been awaiting resolution for well over a year and in some cases two years.

LEGAL COMPLIANCE ISSUES

64. Many of the outstanding issues concerned the drafting and updating of guidance to police forces on the meaning and correct application of PoFA. These issues were discussed at length in my predecessor's last two Annual Reports and are as follows in order of priority:

- Guidance on the treatment of matches against biometric material held unlawfully on the national DNA and fingerprint databases;[62]
- 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;[63]
- Guidance on re-taking fingerprints and DNA samples from an arrested person;[64]
- Guidance on the application of the CPIA exception in respect of DNA samples;[65] and

---

[60] (2008) 48 EHRR 1169

[61] See *Commissioner for the Retention and Use of Biometrics, Annual Report 2015,* at paragraphs 65-93, 214-259 and 262-275.

[62] Ibid at paragraphs 263-267.

[63] Ibid at paragraphs 271-272.

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

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

- Matters arising as a consequence of wrongful arrests and mistaken identity.[66]

65. Satisfactory progress had not occurred in respect of these issues because of an ongoing disagreement between the police service and the Home Office as to which of them should be responsible for providing legal and operational guidance to police on PoFA related issues.

66. I made clear at the beginning of my tenure as Biometrics Commissioner that I considered the situation to be unsatisfactory and against the public interest and urged both parties to resolve these issues as a matter of urgency. A resolution to this problem has now been identified. The Home Office has agreed to seek legal advice, where necessary, and the National DNA Database and Fingerprint Database Strategy Board (NDNAD&FSB) will oversee the drafting and publication of guidance.

67. I would like to thank Carl Jennings and Rod McLean, of the Police Information and Digitisation Unit in the Home Office, for providing the leadership to achieve this progress and Gary Pugh, Chair of the NDNAD&FSB, for agreeing to issue the guidance.

68. Legal advice has been taken by the Home Office on the outstanding legal issues mentioned above. I, however, have not been permitted to see this advice because the Home Office and its legal advisors take the view that such advice is privileged and is for them only. Instead, I have been provided with a summary of the advice drawn up by Home Office officials. Officials also drew up the questions upon which the legal advice was requested. Since I do not have the resource to commission my own independent legal advice I have had little choice but to accept the summaries with which I have been provided at face value and in good faith.

69. The first guidance document on the matter of the treatment of unlawful matches was issued by the Chair of the NDNAD&FSB on 28 February 2017. The remaining legally-based guidance will be discussed initially in early 2017 and guidance should be published in the first quarter of 2017.

70. I will monitor the issuing of this guidance to ensure that these longstanding issues are dealt with. Even if the current timetable is met, updated guidance will be issued almost four years after PoFA was implemented. A way must be found so that if further guidance is needed it can be done at greater pace. As Biometrics Commissioner I am happy to provide good practice advice but to do so I may need either access to the advice of Home Office lawyers or additional resources to commission my own independent advice.

---

[66] Ibid at paragraphs 257-259. See also paragraphs 248 to 250 of this Report below.

TECHNICAL ISSUES REQUIRING LEGISLATIVE CHANGE

CONVICTIONS OUTSIDE ENGLAND AND WALES

71. The 2015 Annual Report detailed the retention regime for individuals convicted of offences outside England and Wales.[67] Biometric material taken from an arrestee cannot lawfully be retained indefinitely simply because the individual in question has been convicted of a qualifying offence outside England and Wales. If the police wish to retain the biometric records of such individuals and have no other basis for doing so, they currently have no option but to go back to those individuals and to take further samples and fingerprints from them.[68] This rule also applies to those convicted of offences in Northern Ireland and Scotland.[69]

72. This problem could only be remedied by way of a change to primary legislation but it had been decided that no such proposal would be included in the Government's 2016/17 legislative programme. Following the submission of the 2015 Annual Report to the Home Secretary in December 2015, however, the Government has reconsidered its position and changes to the regime governing retention of biometrics on the basis of convictions outside England and Wales have been included in the Policing and Crime Act 2017. The relevant provisions should commence in April 2017 and the necessary changes to the PNC and guidance issued to forces by the summer of 2017.[70]

QUALIFYING OFFENCES

73. 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 by section 65A PACE.[71]

74. 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 understand that the relevant secondary legislation is planned for this year, but remains dependent on Ministerial approval.

---

[67] Ibid at paragraphs 68-83. See also Appendix C of this Report.

[68] Ibid at paragraph 70.

[69] Ibid at paragraph 73.

[70] See also paragraph 283-285 of this Report below.

[71] 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

75. 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.[72] This was leading to the unintended automatic deletion of biometrics.

76. The Policing & Crime Act 2017 will pave the way for changes to be made to force custody systems and the Police National Computer (PNC) to enable the police to release arrestees otherwise than on bail whilst an investigation continues without the risk of losing lawfully held biometric material. I understand that the legislation is due to commence on 03 April 2017 and necessary changes to the PNC should be made and guidance issued in time for the commencement of the legislation.

ISSUES RELATED TO THE OPERATION OF PNC

77. In the 2014 and 2015 Annual Reports, a number of matters related to the programming and operation of the PNC were identified and described.[73] I can report that no further PNC issues have been brought to the attention of my Office and that many of the PNC related problems described in previous Annual Reports have now been resolved.

78. Although the majority of PNC issues have been resolved, there remain three areas where I continue to have concerns.

DELAYS IN UPDATING THE PNC

79. My predecessor repeatedly raised concerns about delays and/or errors in updating the PNC with officials at the Home Office, with the NDNAD&FSB and with others and I have echoed those views.[74] 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. As part of the new audit structure discussed above I intend in future to specifically report on force performance in this regard.

---

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

[73] See *Commissioner for Retention and Use of Biometric Material, Annual Report 2014* at paragraphs 212-222; and *Commissioner for Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 220-239.

[74] Ibid at paragraphs 209-211 and 217-219 respectively.

WANTED/MISSING AND LOCATE/INFO MARKERS

80. As reported in previous years,[75] any wanted/missing or locate/info marker placed on a PNC record will prevent the deletion of biometric records even if those records cannot lawfully be retained. In October of 2015 it appears that the biometric records of approximately 4650 individuals were being wrongly retained, as a result of this problem; in 2016 the relevant figure seems likely to have been 8690.

81. Although I understand that it is unlikely that this problem can be wholly resolved, proposed 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 would be substantially reduced (2016 estimates suggest a reduction of approximately 80%).

82. Relevant changes to PNC have not yet been implemented due to preparatory delays by a number of police forces. Indications suggest that the relevant changes to PNC will take effect in early 2017.

BIOMETRICS COMMISSIONER 'UZ' MARKERS

83. 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.[76] This enables me to monitor the number of UZ markers in use and to check the data provided against my own records.

84. As of 02 December 2016, a total of 340 UZ markers were in use by forces in England and Wales. That figure breaks down as follows:

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

[76] Special thanks to Jessica Maltby and Shaun Beresford of ACRO Criminal Records Office for their assistance in collating and reporting the relevant data.

TABLE 12: Biometrics Commissioner 'UZ' Markers by Force (02 December 2016)

Force	No. UZ Applied[77]
MPS	185
GMP	2
Northumbria	11
North Yorkshire	2
West Yorkshire	18
South Yorkshire	2
Humberside	3
West Mercia	5
Warwickshire	1
Derbyshire	1
Cambridgeshire	6
Bedfordshire	6
Hertfordshire	6
Essex	2
Kent	12
City Of London	38
Devon and Cornwall	3
North Wales	2
South Wales	35

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

[77] 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.

i) There have been numerous instances of the inappropriate use of a UZ marker, for example where a police officer has misunderstood the purpose of such a marker or, more commonly, where a UZ marker has simply been erroneously applied.

ii) A common problem is that the retention date associated with a UZ marker on the PNC is incorrect. The cause of this problem seems to be that when a UZ marker is applied to the PNC the 'end date' for retention is automatically set at three years from the date the marker was applied to the record. That end date then needs to be changed manually to reflect the fact that the biometrics can be retained only for three years from the date they were taken.[78]

iii) On a number of occasions UZ markers have been placed on the PNC in order to avoid the inappropriate deletion of biometrics in cases where, notwithstanding the fact that an NFA entry has been made on the PNC, the relevant investigation in reality remains ongoing. Cases of that sort are referred to at paragraphs 75 and 76 above and should be resolved by the proposed changes to the bail process set out in the Policing and Crime Act 2017.

CONCLUSION

86. I shall of course 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 minimize those problems. This will form a key part of my audit process going forward.

[78] 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.

4. APPLICATIONS TO THE COMMISSIONER TO RETAIN BIOMETRICS

4.1 APPLICATIONS TO THE BIOMETRICS COMMISSIONER TO RETAIN BIOMETRICS

87. 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'[79] but neither charged nor convicted.[80] The police must persuade the Commissioner that retaining the biometrics will be useful in the detection, prevention or deterrence of crime.[81]

88. The person who is the subject of such an application must be told on what grounds the application is being made and has the right to make their own representations to the Commissioner challenging the application for retention of their biometrics.[82]

89. 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.[83] 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 C**.

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

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

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

[82] 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.

[83] (See footnote 78)

APPLICATIONS RECEIVED

90. Since the relevant sections of PoFA came into force on 31 October 2013 to 31 December 2016, 386 such applications to the Commissioner were received. Of those 386 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; and
- 177 were made in the period 01 September 2015 to 31 December 2016.

91. Over that latter period, the average rate of applications has remained broadly consistent with that in 2013/14 and 2014/15 at between 9 and 10 per month, even though the number of forces making such applications has increased.

92. 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. In the current (16 month) reporting period (i.e. 1 September 2015 to 31 December 2016), by contrast, 95 of the 177 applications submitted had been from the MPS and the remaining 82 applications had been received from other forces. Whilst it is now the case that 23 of the forces in England and Wales have made one or more applications, 20 forces have yet to make an application – See further Table 13.[84]

[84] City of London Police, Durham Constabulary and Greater Manchester Police have also made applications since 31 October 2013 but not in the current reporting period.

TABLE 13: Number of Applications to the Commissioner by Force (01 September 2015 to 31 December 2016)

Force	Applications
Metropolitan Police	95
West Yorkshire, South Yorkshire & Humberside	25
South Wales	10
Kent	7
Northumbria	5
Cambridgeshire	5
Hertfordshire	5
Essex	5
West Mercia	4
Devon & Cornwall	4
Bedfordshire	3
North Wales	2
Warwickshire	2
Cumbria	1
Derbyshire	1
Dorset	1
Gloucestershire	1
Norfolk	1
TOTAL	**177**

93. In the 38 months since the introduction of the PoFA Regime on 31 October 2013 (i.e. to 31 December 2016), 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 2016	01 September 2015 to 31 December 2016
Total Applications	**386**	**177**
- Representations from subjects	51 (13.2%)	19 10.7%
Concluded by end 2016	**351 (91%)**	**142 (80.2%)**
- Approved wholly or in part	224 (63.8%)	83 (58.5%)
- Refused	85 (24.2%)	47 (33.1%)
- Withdrawn	42 (10.9%)	12 (6.8%)
- Further retention period sought from a District Judge	0	0

STATUTORY BASIS FOR APPLICATIONS TO THE COMMISSIONER

94. 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).

95. Between 31 October 2013 and 31 December 2016, 220 applications were made in relation to victim characteristics and 166 were made for the more general purpose of the prevention or detection of crime.[85] In a number of the former, more than one of the 'victim criteria' were satisfied.

[85] 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.

Table 15: Statutory Basis for Applications to the Commissioner

	Applications received	Approved wholly or in part	Refused
Victim Criteria	**220**	**112**	**64**
- Under 18	194	100	55
- 'Vulnerable'	62	6	3
- Associated with subject of application	13	22	31
Prevention/detection of crime	**166**	**112**	**21**

96. For further statistics on the basis for applications see **Appendix D.**

4.2 PRELIMINARY APPLICATIONS, INTERIM NOTIFICATIONS AND ONGOING COMPLEX INVESTIGATIONS

PRELIMINARY APPLICATIONS

97. 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.

98. In fact matters of disclosure have arisen only relatively rarely and to 31 December 2016 only 6 such applications have been made and all bar one have gone on to become full applications.

INTERIM NOTIFICATIONS

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

100. 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'.[86]

101. 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 2016 my Office was informed of 114 Interim Notifications. As at that latter date, 20 of those Notifications had been followed by applications under section 63G and 76 had 'lapsed' either because (in 61 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 15 cases) it was decided not to proceed to a full application.

ONGOING COMPLEX INVESTIGATIONS

102. My predecessor's 2015 Report[87] 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.

103. My Office is aware of a number of investigations of this sort and receives regular monthly updates on the cases concerned. As explained at paragraphs 75-76 above, the issues in respect of biometric retention in complex and protracted investigations should be mitigated by the changes to the legislation governing police bail contained in the Policing and Crime Act 2017.

---

[86] 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.

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

4.3 APPLICATIONS TO A DISTRICT JUDGE (MAGISTRATES' COURT)

104. 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.[88] 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.[89]

105. Biometric material held following a successful application to the Commissioner has only recently come to the end of the initial three year retention period. By the end of 2016 the biometrics in 18 cases were eligible for an application to a District Judge under section 63F of PACE but no such applications were made. It is not possible to predict to what extent such applications will be made in the future.

106. As regards individuals who have been charged with (though not convicted of) qualifying offences, however, it has since 31 October 2013 been open to the police to make applications for a further two years to a District Judge.[90]

107. In the event only 6 such applications had been made to District Judges by 31 December 2016 and all of them were made by the MPS. Only 4 of those 6 applications were successful and in each of them the District Judge gave detailed reasons for his or her decision.

4.4 ISSUES ARISING FROM RETENTION APPLICATIONS TO THE COMMISSIONER

108. The applications received since the commencement of the relevant sections of PoFA have raised a number of questions which are discussed below.

WHY ARE SO FEW POLICE FORCES MAKING APPLICATIONS?

109. 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 judgment and forces have differed in their conclusions.

---

[88] (See also footnote 78)

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

[90] (provided that the relevant DNA profiles and/or fingerprints would otherwise have been subject to automatic deletion on or after 31 January 2014)

110. Some forces have established dedicated units to review possible cases and then make applications whilst others have left the responsibility of making applications to the initiative of individual investigating officers. As we have seen from the example of the Metropolitan Police Service's Biometric Retention Unit, the former approach is more likely to generate a regular flow of applications. The Metropolitan Police were the first to set up a separate unit and were responsible for almost all early applications received.

111. Applications from non-Metropolitan forces started later because it was only from November 2015 that the Police National Computer (PNC) was capable of identifying NFA cases where an application could be considered. There is no such corresponding method identifying cases suitable for application to a Magistrate's Court or District Judge under section 63F of PoFA.

112. At present not all forces are making applications under section 63G of PoFA (see Table 13) although I understand that some additional forces are considering doing so.

113. It should be noted that whilst the present rate of applications enables me to respond within a reasonable period, this might not be possible if the application rate were to significantly increase. If all forces in England and Wales decided to make applications the number of cases could feasibly double.

HOW ARE APPLICATIONS MADE AND PROCESSED?

114. In practice the police make applications to the Commissioner on a standard pro-forma 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 they have put forward in the application. This proforma must be authorised by a Chief Officer of Police and is usually submitted to my Office electronically.

115. The Office's casework staff check that the application is valid with reference to the PofA provisions, summarise the case being made and, on that basis, formulate a recommendation as to whether a necessary and proportionate case for retention has been made. I receive that summary but also have direct access to the whole of the case file in order to check or flesh out any part of the summary about which I am uncertain. Each case can then be discussed with the caseworker before I reach a decision. Forces are then told what the decision is and, if the case is refused, the reasons for that refusal.

116. In every instance, the subject of an application is told if that application has been rejected 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.[91] 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.

117. 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.

118. All correspondence is sent by Royal Mail 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?

119. In order to make an application the police have to demonstrate that, whilst the subject was not charged, there is evidence to show that it is likely that the subject of the application was involved in the act, that holding the biometrics 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'*.[92] Furthermore, and as was contemplated by section 24 of PoFA, formal guidance about such applications has been published by the National DNA Database Strategy Board.[93]

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

- the available evidence is unlikely to support a successful prosecution;[94] or

[91] 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.

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

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

[94] 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

- charging the subject would not be in the public interest.[95]

121. If the former, the subject of an application may regard it as strange that where there is insufficient evidence to justify charging there can be sufficient grounds to justify retention of 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 the criteria as set out in the 'Principles' document are satisfied and that retention of the subject's biometrics is considered 'appropriate'.

122. 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.

123. 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 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.

124. 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.

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

WHAT TYPES OF OFFENCES LEAD TO APPLICATIONS?

126. Only 'qualifying offences' can be the basis of an application but, as can be seen in Table 16, the majority (63%) of applications are for sexual offences.

---

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.

[95] 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.

TABLE 16: Outcome of Applications to the Commissioner to Retain Biometrics for Qualifying Offences under section 63G PACE (31 October 2013 – 31 December 2016)

Offence Group	Total Applications	Approved	Refused	Withdrawn	Yet to be Decided
Murder, Attempts and Threats to Kill	7	5 (71%)	2 (29%)	0 (0%)	0 (0%)
Sexual Crimes	246	128 (52%)	70 (28%)	23 (9%)	25 (11%)
Assaults	66	45 (68%)	8 (12%)	10 (15%)	3 (5%)
Robbery	44	32 (73%)	1 (2%)	7 (16%)	4 (9%)
Burglary	18	12 (67%)	5 (28%)	0 (0%)	1 (5%)
Other	9	5 (56%)	0 (0%)	2 (22%)	2 (22%)
Total	**390**	**227**	**86**	**42**	**35**

127. The high percentage of sexual offences seen to date is probably because the handling of allegations of sexual crimes has been controversial for some time. Often there are no witnesses and so 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.

128. 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 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.[96] Conversely, the guidelines also advise that it may not be in the public interest to criminalise sexual behaviour, especially between young people[97], 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

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

[97] 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.

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.

129. 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.

130. 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.

131. There is a general belief amongst the police, however, that minor sexual offending, or familial sexual offending, will lead to more serious sexual offending or stranger attacks. There is some evidence to support this belief but it is by no means conclusive[98] and in any case the evidence refers to overall statistics and does not provide a basis for predicting the future behaviour of an individual.

132. 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 and I must make the best decision we can on the basis of the facts in each individual case.

133. Since the first applications to the Commissioner under section 63G to be approved were in relation to material taken in November 2013, over the coming months and going forward it is my intention to examine the rate of conviction for subjects during the 3-year period that their biometrics are retained.

---

[98] 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

WHY DO SO FEW SUBJECTS OF APPLICATIONS MAKE REPRESENTATIONS?

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

Table 17: Representations by Subjects and Outcomes (31 October 2013 – 31 December 2016)

Applications	Totals	Representations
Approved Applications	224	24 (11%)
Refused Applications	85	19 (22%)

135. 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.

136. Most forces do this by providing the subject with a copy of the application form which they have submitted to my Office. In a small number of cases I have formed the view that, because of the limited disclosure that had been made to the subject by the applying force, it would be inappropriate for me to attach any weight to a point or points raised in the application form. In 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. In none of those cases so far, however, would my decision have been different if proper information had been provided to the subject. 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.

137. 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.[99]

[99] See paragraphs 97-98 of this Report above.

138. Notwithstanding issues of disclosure, I do not believe that the format of the notification letter or the few examples of inadequate notification are reasons 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.

139. 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. More worrying is if subjects believe that they will not be listened to or that they simply wish, following an NFA for a serious offence, to bring to an end what has been a lengthy and stressful experience.

140. Whatever the reasons for the low submission rate, I intend to look into the matter further over the coming months.

4.5 THE TREATMENT OF CHILDREN AND YOUNG PEOPLE

141. 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*."

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.

142. 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.

143. 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 that child or young person understands their rights to make representations.

144. In December 2016, I discussed the problem with Chief Constable Olivia Pinkney, the National Police Chiefs' Council 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 National Police Chiefs' Council.

145. 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 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. I am grateful to Chief Constable Pinkney, for her support and for agreeing to develop a new approach.

4.6 EXTENDING THE QUALIFYING OFFENCES LIST

146. 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'. The previous Commissioner drew attention to the fact that the list of 'qualifying offences' excluded both some very similar offences and equally serious offences to those already featured on the list.[100]

147. The Home Office has been considering extending the list of qualifying offences and may do so shortly.[101] This would certainly be logically neater, although it should be noted that the changes are being considered before the utility of the section 63G application process has been evaluated.

148. 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 the proposed option.

---

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

[101] See paragraphs 73-74 above.

5. BIOMETRICS AND NATIONAL SECURITY

5.1 POLICE BIOMETRICS AND NATIONAL SECURITY DETERMINATIONS

149. As well as introducing stricter rules as regards the retention by police in England and Wales of biometric material which has been obtained from unconvicted individuals, 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 of national security interest and that cannot lawfully be retained on any other basis.

150. A responsible Chief Officer or Chief Constable[102] has the power under PoFA to order that 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.

151. An NSD must be in writing and lasts for a maximum of 2 years beginning with the date it is made. [103] 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 E**.

5.2 COUNTER-TERRORISM DATABASES

GENERALLY

152. Biometrics retained under an NSD are held on separate counter-terrorism DNA and fingerprint databases,[104] administered by Secure Operations – Forensic Services of the Metropolitan Police (SOFS). All new DNA profiles and ten-print fingerprint sets which are loaded to the NDNAD and IDENT1 are checked against those CT databases.[105]

153. 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 October 2016 was some 9,086. Those latter figures encompass

---

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

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

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

[105] 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.

both new additions to the databases since 31 October 2013 and deletions from those databases after that date.

154. Of the individuals whose biometric records were being held by the police on those databases as at 31 October 2016 some 1,250 (i.e. about 14%) had never been convicted of a recordable offence.

TABLE 18: Holdings on the CT Databases[106]

		2013[107]	2015[108]	2016
DNA	**DNA**			**608**
	- Of which unconvicted			65 (11%)
Fingerprints	**Fingerprints**			**8,478**
	- Of which unconvicted			1,185 (14%)
TOTALS	**Total Holdings**	**8,300**	**9,600**	**9,086**
	- Of which unconvicted[109]	4,500 (54%)	5,050 (53%)	1,250 (14%)
	- *New material*[110]			*695 (56%)*
	- *Legacy material*[111]			*555 (44%)*

(Source: SOFS)

155. As at 31 October 2016, the majority (93%) of CT biometric holdings were for fingerprints. This reflects the fact that fingerprints have been in use for much longer than DNA and because fingerprints are more easily, quickly and cheaply checked against police databases they are more commonly used to establish identity. The same is true for non-CT police use of such biometrics.

---

[106] CT Database figures are not available for 2014 – see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2014* at section 3.

[107] Breakdown unavailable due to transition to a new Management Information system.

[108] (see footnote 107 above)

[109] The figures stated for 2013 and 2015 do not take account of additional legacy records discovered after April 2016.

[110] Additions to the CT databases since 31 October 2013.

[111] Biometrics held on the CT databases before 31 October 2013.

156. By October 2016 the percentage of overall data held on the CT databases for unconvicted subjects was lower because during that year all remaining legacy cases were reviewed and either made PoFA compliant, through the making of NSDs, or were deleted/destroyed.[112]

GOVERNANCE

157. Physical separation of the Counter Terrorism DNA Database (CTDNAD) from the NDNAD was implemented as a simple way to limit and control access to such highly sensitive information. More modern databases achieve such control not through physical separation but logical separation by design with different access, business and governance rules within a single database framework. Access control assurance can be provided for the latter through audits to show who has had access to which data, when and for what purpose.

158. The NDNAD&FSB has endorsed proposals for the NDNAD to move to logical separation control as part of the Home Office's biometric plans to update the database.[113] I am yet to be persuaded as to why the CTDNAD should be administered by different organisations once such logical separation control is possible.[114] I have suggested to the NDNAD&FSB that the effectiveness of such logical control and the attendant governance and audit framework and their ability to meet the more stringent requirements of the CTDNAD should be demonstrated before such a move occurs.

159. My predecessor reported that the CT databases suffer a 'governance deficit' as regards the comprehensive governance arrangements and protocols that might be reasonably expected.[115] Since taking up post in June 2016, I have reiterated to those concerned the importance of 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 as a matter of some urgency. I understand that proposals are to be discussed by the NDNAD&FSB in March 2017. I consider this area to be a key priority for the coming year.

160. 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

---

[112] Special thanks to staff within Special Operations Forensic Services at the MPS for their help in compiling the relevant data and for their assistance during the 2015/2016 reporting year.

[113] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 319-322.

[114] See paragraphs 11 to 14 of this Report. The CT Fingerprint Database is a separate database cache within IDENT1. Both the CT DNA Database and the FP Database within IDENT 1 are administered by SOFS. See also *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraph 167.

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

non-law enforcement agencies, such as the security and intelligence services. Law enforcement bodies for these purposes are defined in PoFA[116] and have access to the counter terrorism biometrics databases.

5.3 THE NSD PROCESS

161. As explained above, deciding whether an NSD should be approved is a matter for Chief Officers of police.[117]

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

163. Initially applications to Chief Officers for NSDs are put together either by the Joint Forensic Intelligence Team (JFIT) in SO15 or PSNI. PSNI deals with all Northern Ireland cases but JFIT oversees all other cases and most of those are signed off by a Metropolitan Police Commander. Applications for biometrics taken by regional CTUs are signed off by their respective Chief Officers.

164. The information on which NSD applications are made is largely drawn from police records of previous criminal justice system contacts and police intelligence. In some cases additional information will come from the Security Service, who will provide additional supporting data for retention.

165. If it is decided that an NSD application should be made, the supporting data is summarised on the application form and sanitized where necessary. 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. JFIT/PSNI add a reasoned recommendation to the application which also proposes to the Chief Officer whether it judges that the supporting intelligence/evidence is adequate to grant an NSD. There is Statutory Guidance on what should be considered, further discussion of which can be found in **Appendix E**.[118]

---

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

[117] 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.

[118] See also *Protection of Freedoms Act 2012: Guidance on the making and renewing of National Security Determinations allowing the retention of biometric data.*

166. 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.

167. If an application for an NSD is approved, the decision of the Chief Officer is recorded at the end of the application 'form' together with his or her reasons for approving the application. That document then becomes the NSD and the NSD IT System automatically forwards it to my Office for my review. My Office also receives copies of any applications that are refused by Chief Officers.

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

ROLE OF THE RESPONSIBLE CHIEF OFFICER

169. An NSD may only be made or renewed by a responsible Chief Officer or their nominated deputy.[119]

170. 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.

171. Like my predecessor, I have been generally impressed with the care taken to identify the cases for which an NSD might be properly considered and similarly with the decision making process as to whether an NSD should be made. By no means all possible cases are considered for an NSD and not all of those put forward are accepted by Chief Officers demonstrating that, in the vast majority of cases, proper judgment is being exercised.

THE ROLE OF THE COMMISSIONER

172. Once a Chief Officer has decided an NSD, the NSD IT system automatically informs my Office. My job as regards NSDs is laid down in PoFA as 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.

(http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf)

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

If I do not think that retention of the relevant material is necessary or proportionate I have the power to order its destruction.[120] This is a significant power which, given the threats being managed, I should exercise carefully.

COMMISSIONER'S REVIEW OF NSDS MADE OR RENEWED

173. 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. If I did so there would be little point in Chief Officers making their determinations. Chief Officers are better placed and more experienced in deciding matters of national security than me. Rather, my role is to examine each application to ensure that the evidence exists on which a 'reasonable Chief Officer' could have granted an NSD.

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

175. As can be seen in Table 19 below, of the 591 NSDs made by 31 December 2016, I had completed my review of all 591 by that date. I had raised challenges in 96 (16%) of cases I examined and in 42 (44%) of these I ordered the destruction of biometric material since I was not persuaded by the police response to my challenge.

176. It is perhaps not surprising that the majority of the challenges raised have related to pre-PoFA Legacy cases since these could be several years old. Whilst the passage of time may not change the strength of the evidence originally used to justify retention of the biometrics, it is important that the threat assessment is brought up to date. Whilst challenges may be more likely for legacy cases they can, and have, occurred in relation to applications for new material.

177. Most of the challenges I have made have been because either I had doubts as to whether the case presented offered a current threat assessment, 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 provide updated supporting data for retention.

---

[120] PoFA Sections 20 (2)(a & b),(4) and (5).

178. 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 for retention.

QUALITY OF NSD APPLICATIONS

179. The previous Commissioner worked with JFIT to ensure that the pro-forma used for NSD applications is laid out in such a way to ensure that the case for necessity and proportionality is properly addressed and generally this is the case.

180. However, I have concerns that in a small number of cases applications are over-formulaic and sometimes confuse the case for holding an intelligence file on a subject with the specific case to retain biometric material. I have discussed these concerns with representatives of JFIT and they have undertaken to do further work to ensure that all applications make the specific case for the necessity and proportionality of retaining biometric material.

181. 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.[121] JFIT/PSNI present the available evidence/intelligence to Chief Officers in a thorough manner and Table 19 below shows that Chief Officers are exercising their judgment when deciding whether or not to make an NSD.

THE USE TO WHICH NSD MATERIAL IS PUT

182. 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 that material is being used otherwise than for permitted purposes. However, the transitional legacy workload (see below) has limited the time that could be spent on this second requirement. 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 records of the use of retained material.

---

[121] 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)

5.4 LEGACY MATERIAL AND NEW MATERIAL

183. 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).

LEGACY MATERIAL

184. Prior to 31st October 2013 biometrics were taken for national security purposes under a number of legislative provisions and generally retained indefinitely regardless of whether the individual concerned had been convicted of an offence.

185. By section 25 of PoFA the Secretary of State was required to make an order prescribing appropriate transitional procedures as regards Legacy Material[122] and by such an Order[123] 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.

186. The previous Commissioner reported[124] that, due to resourcing restraints and other reasons, JFIT had failed to assess these legacy records within the timescale laid down by the original Transitional Order and that a large number of those records would have been destroyed had Parliament not agreed in October 2015 a one year extension of that transitional period until 31 October 2016. [125]

NEW MATERIAL

187. For New Material, 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

---

[122] (i.e. material taken before 31 October 2013). Material taken after 31 October 2013 is hereafter referred to as 'New Material'.

[123] 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).

[124] *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at paragraph 137

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

arrested or detained without charge, the relevant retention periods in the absence of an NSD are summarised at **Appendix E**.

5.5 CASES REVIEWED AND NSDS MADE

188. By 31 December 2016 the cases of approximately 5,800 individuals who had never been convicted of a recordable offence but whose biometric records were nonetheless being retained on the national CT databases had been reviewed by JFIT/PSNI for NSD purposes.[126]

TABLE 19: NSD decisions year ending 31st December 2016

Total Possible NSDs applications processed	**713**
- NSDs approved by Chief Officer	591
- NSDs declined by Chief Officer	122
- NSDs supported by Commissioner	543
- NSDs challenged or further information sought	96
- NSDs upheld by Commissioner but with reservations	6
- Destruction ordered by Commissioner	42

5.6 NSD ISSUES

ISSUES AFFECTING NEW MATERIAL

189. A number of IT issues, procedural errors and handling delays emerged during the extension to the Legacy period which 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. My predecessor provided a Further Report to the Home Secretary on these matters in April 2016[127] and the Commissioner's staff has worked closely with Metropolitan Police's

[126] Special thanks to staff within JFIT/PSNI for their help in compiling the relevant data and more generally for their assistance during the 2015/2016 reporting year.

[127] See *Further Report by the Biometrics Commissioner on issues raised in his 2015 Annual Report*, April 2016 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/526235/55843_Biometrics_PRINT.pdf)

Counter-Terrorism Command to ensure that these problems were systematically addressed and appropriate mitigatory action taken.

190. Since the publication of that Further Report, the new biometrics of 13 additional individuals have been lost. The biometrics of 9 of those 13 were lost because JFIT failed to sequence the work so that cases were assessed before the relevant biometrics reached their statutory deletion date. The biometrics of the remaining 4 individuals were lost due to administrative errors within JFIT and/or SOFS. I am satisfied that measures have now been taken within JFIT/SOFS to remedy the causes and mitigate the effects of these problems where appropriate. I can report that no biometric material has been lost since July 2016.

ISSUES AFFECTING LEGACY MATERIAL

191. In his further Report in April 2016, the previous Commissioner noted that due to issues with the IT application used by SOFS to manage the CT databases, approximately 1,800 additional Legacy records had been discovered which had not previously been accounted for.[128]

192. Since I have been in post, a full audit of the IT application used by SOFS uncovered approximately 950 further additional Legacy records which had previously been overlooked. All of these records were reviewed and, where appropriate, NSDs applied for prior to the expiry of the transitional period.

193. In July 2016 a further 44,000 paper hardcopy fingerprint legacy records were discovered by the Metropolitan Police. However, since these were records of some age, it was believed that all of those taken by police forces from England, Wales and Scotland – approximately 25,000 records - had either been uploaded to the national collection on IDENT1 and deleted under the cleansing exercise prior to the commencement of PoFA or were also held in a digital format in compliance with PoFA in the national and/or CT fingerprint database within IDENT1. To verify this, I asked that a sample of 200 records, chosen at random, be examined and this provided statistical re-assurance at the 95% confidence level that the records had been properly dealt with.

194. 19,000 of the 44,000 paper hardcopy fingerprint legacy records recently discovered related to material taken by the Royal Ulster Constabulary in Northern Ireland and have now been transferred back to the Police Service of Northern Ireland (PSNI).[129]

---

[128] Ibid at paragraph 33.

[129] (see also paragraphs 196 to 199 below)

195. With the exception of the aforementioned Northern Ireland records, the assessment of all Legacy records was completed on time by the 31 October 2016. SOFS, JFIT and Commander Haydon must be congratulated on dealing quickly with such a large body of cases.

5.7 NSDS IN NORTHERN IRELAND

196. 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.[130] This Order applies only to Northern Irish biometric material 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"*.[131]

197. 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 the Historical Investigations Unit has identified which biometrics may be needed. I understand that the aforementioned 19,000 hardcopy Legacy fingerprint records will be reviewed as part of that process.

198. Nevertheless, a number of legacy cases were reviewed and a small number of NSDs made prior to the parliamentary extension being granted. I have advised the PSNI that these NSDs, once made, are now subject to the PoFA bi-annual renewal requirement and cannot be put back into the pot of legacy cases that need not be reviewed until 31 October 2018.

199. 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.

5.8 ASSURANCE AS REGARDS LEGACY HOLDINGS AND NSD ISSUES

200. The completion of the comprehensive review of Legacy material for England, Wales and Scotland provokes a number of questions which I have raised with the Counter Terrorism Command as regards the NSD process:

---

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

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

i) What assurance can be given that all Legacy cases have now been identified and dealt with?

ii) What governance arrangements have been put in place for the future to avoid such problems?

iii) Given that the management of legacy cases led to a very large spike in the number of NSD cases in the last 12 months that both a Chief Officer and the Commissioner had to examine; how will these cases be managed as they come up for possible renewal in two years time?

201. Commander Dean Haydon, of the Counter Terrorism Command, has written to me answering each of these questions.

202. I am satisfied that all CT biometric holdings have now been thoroughly checked and verified. The database used by the Counter Terrorism Command and the underlying database run by the MPS's Directorate of Forensic Services (HAILOH) have now been cross checked and this will continue on a quarterly basis to provide ongoing re-assurance. The Directorate of Forensic Services has also reviewed the operations of their HAILOH records management system and some modifications have been made to avoid any repeat problems.

203. As regards governance, in future the PoFA CT Programme Board will report to a National Security Biometrics Board, chaired by Commander Haydon. In practice this is a higher level of accountability than applied in the past and will apply performance management indicators to monitor performance. Furthermore, the CT biometric databases will come under the NDNAD&FSB as do the other fingerprint and DNA databases. This is a more structured governance framework than existed in the past and I shall examine how well it works in the future.

204. Since all Legacy material had to be brought within the PoFA retention regime by the end of October 2016 and due to the numerous issues that have come to light in the last 12 months, there was a very significant spike in the number of NSD applications determined by Chief Officers in the latter part of 2016. In the 6 months to 31 October 2016 some 5,588 cases were reviewed. That spike could have been repeated bi-annually and at the same time the Northern Ireland legacy cases would be due to be brought within PoFA. However, Commander Haydon informs me that re-applications for existing NSDs will be staggered throughout the coming year to avoid a single annual spike.[132]

[132] I understand that PSNI are considering a similar approach.

5.9 OTHER MATTERS

FUTURE NSD WORK LOAD

205. 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. 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[133] should be reviewed regularly and independently overseen.

206. NSDs will be reviewed frequently 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. However, to introduce further additional retention periods to the various schemes already in use would make the process of making and renewing NSDs even more complex and, therefore, potentially more prone to error. The requirement for frequent reviews for all NSDs has the advantage of simplicity and ensuring that evidence exists that they remain proportionate and necessary.

PRE-EMPTIVE NSDS

207. In his 2015 Annual Report, my predecessor detailed the problems which had arisen in relation to biometric material taken under PACE provisions and retained for the purposes of national security.[134] With the recent large throughput of NSDs, another unfortunate PACE-related feature of applying for NSDs has become apparent.

208. 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.[135] 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.

209. 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

---

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

[134] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 147-151.

[135] See paragraph 43 of this Report above.

national security concern has been arrested but the result of the further investigation is still unknown.

210. These are pre-emptive NSD applications which 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 justificatory evidence already exists.

211. A related issue regarding individuals arrested otherwise than under Section 41 TACT is that there is often a delay in notifying JFIT and SOFS 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. JFIT and SOFS 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 JFIT/SOFS 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. JFIT and SOFS 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.

212. The most straightforward solution to these problems 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 the Commissioner to retain the biometrics for qualifying offences and a similar period for NSD applications would avoid the need for pre-emptive NSD applications.

213. 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 I have asked them to consider doing so urgently. If they do not do so I have indicated that I shall be obliged to reject any pre-emptive NSDs without the necessary justificatory evidence.

NSDS: 'MATERIAL' VERSUS 'INDIVIDUAL'

214. 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. I intend to discuss this problem with OSCT to see if a practical solution can be found.

6. DELETION OF BIOMETRIC RECORDS

6.1 DNA SAMPLES

BACKGROUND

215. There are clear rules in PoFA as to when biometric samples should be deleted.[136] 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. Police are, however, allowed 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 (CPIA). This is one of the areas on which my predecessor called for clearer guidance to be issued and to which Ministers agreed that *"further guidance on this issue would be beneficial"*[137] although it is yet to be produced. The Home Office has taken legal advice on the issue and has undertaken to produce that guidance within the year.[138]

216. The majority of DNA samples taken for PACE or elimination purposes are passed 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.

217. As stated earlier[139] my Office, in collaboration with UKAS, has responsibility for the oversight of the implementation and operation of the biometric retention regime introduced by PoFA. It is my intention over the coming months to further expand these oversight activities in terms of data collection and analysis to give a broad picture of force activities in this regard.

HAVE DNA SAMPLES BEEN APPROPRIATELY DESTROYED?

218. From oversight activities and visits carried out to date, neither I nor my predecessor have found reason to suspect that (and save only in reliance on the CPIA exception discussed 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.

---

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

[137] Ibid at paragraph 181.

[138] See paragraphs 64-70 of this Report above.

[139] See paragraphs 53-59 of this Report above.

CPIA EXCEPTION

219. 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 is 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"*.[140] 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. [141]

220. Since January 2016 all DNA samples, which are held under CPIA beyond 6 months from the date they were taken, are required to be reviewed on a quarterly basis by the responsible police force.

221. It is clearly open to forces to take differing views as to the circumstances in which a DNA sample "*is, or may become, disclosable"* under the CPIA or any relevant code of practice – and it seems equally clear that forces in fact do so. In some cases this can mean that samples are held for a long time: for example, where a case results in a long prison sentence, an arrestee or elimination sample used in evidence must be held against the possibility of an appeal or an investigation by the Criminal Case Review Commission until the completion of the sentence.[142]

NUMBERS

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

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

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

---

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

[141] 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.

[142] See CPIA Code of Practice, at paragraph 5.9 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf)

223. The NDNAD Delivery Unit (the 'NDU') has continued to provide me with monthly schedules based on returns made by FSPs and police forces. The figures given in those schedules include both arrestee samples and elimination samples and the relevant figures are (so far as is possible) broken down by force. Each month those schedules provide the numbers of such samples that are being held by FSPs on behalf of forces; every three months those schedules also provide details of the numbers of such samples that are being held 'in force'. Those schedules can at best provide me with only an approximate picture of the position as regards the retention of samples pursuant to the CPIA exception as samples are retained and destroyed on a near constant rolling basis.

224. It should also be noted that the quarterly returns for in-force holdings received by the NDU are partial. A significant number of forces have failed to provide figures or are simply unable to do so because they do not have centralised systems for monitoring in-force holdings of DNA samples. This situation is at best unsatisfactory and at worst could indicate that certain forces are not complying with PoFA with regards to the review and destruction of DNA samples held under CPIA. This is a matter in relation to which I intend to issue best practice guidance in 2017.

225. 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 2016. These are set out below in (Table 20).

TABLE 20: DNA samples held under CPIA as of 31 December 2016

	Total	Held in Force[143]	Held by FSPs
Arrestee Samples	4,797	58	4,739
Elimination Samples	14,596	2,775	11,821

(Source: National DNA Database Delivery Unit)

ELIMINATION SAMPLES

226. Since January 2016, all elimination samples, i.e. samples taken from – and with the consent of – third parties in connection with the investigation of an offence, have been subject to the same retention rules as those taken from individuals arrested for recordable offences. All samples must be deleted within 6 months or as soon as a profile has been derived save those held under the CPIA exception. All DNA samples held within forces or with FSPs must

[143] Only 11 England and Wales forces reported on their holdings of elimination samples. Similarly only 14 out of 43 forces reported on their holdings of Arrestee samples.

be reviewed on a quarterly basis to ensure that their continued retention is necessary and proportionate.

227. In January 2016 new consent forms were introduced in relation to the taking of volunteer DNA samples for elimination purposes. All volunteers who provide volunteer samples for elimination purposes must sign a relevant consent form which explains their rights, how the DNA sample they provide will be processed and how the resulting information will be stored and used. In the case of young people, under the age of 18 years, there is a general provision that the consent should be countersigned by a parent, guardian or responsible adult.

'GILLICK COMPETENCE'

228. In December 2016, my Office received a query from Lancashire Police and the Dean at the Faculty of Legal Medicine at the Royal College of Physicians to provide advice on an issue which had arisen in relation to the profiling of DNA elimination samples.

229. The issue had arisen where DNA elimination samples had been taken from young people, under the age of 18 years, but the associated paperwork had not been countersigned by a responsible adult. The police had reported that in some cases FSPs had refused to profile the elimination samples due to the lack of a counter-signature. These situations had generally arisen in instances when a young person had been the victim of a serious and/or sexual crime and had attended a Sexual Assault Referral Centre (SARC) without a responsible adult. The young person had not wished for their parent or guardian to be informed of the crime and would not have attended the SARC if it were likely that their parent or responsible adult would have been informed. These individuals had had elimination samples taken as they had been considered 'Gillick Competent'[144] by those taking the samples; however, the associated paperwork had not been countersigned.

230. I referred the matter to the National DNA Database Ethics Group and they agreed that FSPs should be profiling these elimination samples when appropriate to do so. However, they acknowledged that FSPs needed to be cognisant of the law and that the lack of a counter-signature on an elimination form could raise questions for the FSPs as to whether they were able to legally process the sample. It was suggested that relatively minor changes to the

---

[144] The term derives from the caselaw of *Gillick v West Norfolk* [1984] Q.B. 581, 597, and later upheld by the House of Lords [1985] UKHL7, where Mr Justice Woolf stated:

"...whether or not a child is capable of giving the necessary consent will depend on the child's maturity and understanding and the nature of the consent required. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the treatment proposed, so the consent, if given, can be properly and fairly described as true consent."

elimination consent form would address the issue and FSPs should be made aware that it was not mandatory for elimination consent forms to be counter-signed.

231. My Office has been in discussion with the NDU since that meeting with a view to updating guidance to forces and FSPs. I understand that a memorandum to all forces and FSPs has been circulated in advance of formal changes being made to the format of the relevant consent forms and to national guidance.

ARRESTEE SAMPLES

232. The current Home Office guidance to forces on the application of the CPIA exception states:

> *"It is expected that in the great majority of cases, PACE samples will be destroyed either as soon as a DNA profile has been derived or, if sooner, within six months of the sample being taken."*

233. Given the relatively small number of arrestee samples that are apparently being retained, it seems that forces are attempting to act in accordance with that guidance and that they are giving careful thought to the retention of arrestee samples on that basis. As previously reported[145] forces have continued to take differing views of the true scope of that exception and some forces continue to retain many more arrestee samples than other forces. Consequently, in the course of my visits to forces, I have undertaken specific checks on their activities and policies as regards the retention of DNA samples in reliance on the CPIA exception.

234. This reporting period, my office has visited Hampshire Constabulary, Kent and Essex Police Collaboration, Cambridgeshire Constabulary, Cumbria Police, Devon, Cornwall and Dorset Police Collaboration and West Midlands Police. Overall, I have been impressed by the openness which forces have shown my staff during those visits and by their readiness to share information. During the visits, my staff have found many instances of good practice and that real efforts have been, and are being, made by the forces visited to ensure full compliance with the PoFA regime. It was found, however, that some forces were more advanced in this process than others.

235. I am also satisfied that where deficiencies or gaps have been identified in force processes, the forces affected recognised those deficiencies and have taken or are taking relevant steps to mitigate their effects and remedy those issues.

236. It was found that a small number of the forces visited do not have a centralised process for the monitoring and review of DNA samples held in force. In these forces, the retention and

---

[145] See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at paragraphs 171-210.

review of DNA arrestee and/or elimination samples under CPIA is left to individual investigating officers to manage and holdings are not reviewed centrally. For each of these forces, a recommendation has been issued that centralised processes should be devised and implemented as a matter of some urgency to ensure that the forces are fully compliant with the requirements of PoFA.

DE-LINKED' ARRESTEE SAMPLES AND CPIA

237. Forensic Service Providers (FSPs) process PACE DNA samples on behalf of police forces, although the Chief Officers of those forces remain the legal owners and data controllers of those DNA samples and the DNA profiles which are derived from them.

238. In July 2016, it was brought to my attention that 448 DNA samples which had been 'delinked'[146] by an FSP were being retained under the CPIA exception on the request of police forces even though the corresponding DNA profiles were no longer held on the NDNAD. This situation has a two-fold effect:

    i) Once delinking has taken place, the continuity and audit trail for the sample retained under CPIA is no longer complete as the DNA sample can no longer be definitively linked back to the DNA sample barcode on the FSP information management system;

    ii) The continued retention of these samples under CPIA goes against the principles of the delinking process. Once the sample has been retrieved it could be possible to manually link this back to the delinked DNA profile on the FSP information management system.

239. I have made clear to the FSP concerned and to the National DNA Database Delivery Unit that such samples should not be retained after the corresponding profile has been deleted from the NDNAD and that the retained DNA samples already identified should be destroyed. This issue has subsequently been raised at the National DNA Database and Fingerprint Database Strategy Board and with force representatives to determine the reasons for requests for continued retention under CPIA. I shall continue to keep this matter under close review.

CONCLUSION

240. In summary, save only that some samples stored in-force may not be reviewed as frequently as required and that, due to differing interpretations of the provisions, the CPIA exception

[146] De-linking is the process whereby the link between a DNA profile and its associated demographic information is broken on the FSP Information Management System meaning that, after a DNA profile is deleted from the NDNAD, the DNA profile cannot be linked back to the DNA sample from which it was derived or the demographic details of the person from whom the DNA sample was taken.

may sometimes be being misapplied, I have found no reason to suspect that there has been significant non-compliance with either the sample destruction regime provided for by PoFA or the CPIA exemption. It seems clear, however, that forces differ substantially in their approaches to the CPIA exception and not all forces rigorously comply with their obligation to destroy both arrestee and elimination samples as soon as the CPIA exception ceases to apply.[147]

6.2 DNA PROFILES AND FINGERPRINTS

241. The previous two Annual Reports discussed a number of problems with the proper deletion of DNA profiles and fingerprints as required by PoFA. Many of these remain and will be covered by guidance to be issued by the NDNAD&FSB in early 2017 (see section 3 of this Report).

COPIES

242. 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).

243. As regards copies of DNA profiles and fingerprints, I have little to add to the observations made at paragraphs 246-250 of my predecessor's 2015 Report. 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.

244. 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 being retained.

245. My Office made a return visit to the National Fingerprint Archive in April 2016 and was once again impressed by the care which is taken by its staff to ensure that hard copy fingerprints which should have been destroyed are not released to requesting forces.

246. Following my predecessor's previous visit in May 2015 various recommendations were made to them 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

[147] (see footnote 140 above).

Archive provides regular performance statistics on its operations to my Office on a quarterly basis.[148]

TABLE 21: Deletions from National Fingerprint Archive (January - December 2016)

	All Forces
Total PoFA deletion notifications received from IDENT1	**42,111**
Hardcopy records found and destroyed	7,281
No. of hardcopy records held in National Collection	34,357
Requests received from other police forces where ten-print records were found and destroyed[149]	147

(Source: National Fingerprint Archive)

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

6.3 DELETION OF BIOMETRICS ORDERED BY CHIEF OFFICERS

248. People whose biometrics are being lawfully retained by the police can apply for the 'early' deletion of their records from national police systems.[150] Previous Annual Reports drew attention to the very limited circumstances under which such an application can be made and urged a less restrictive approach.[151]

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

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

[150] Section 63AB of PACE (as introduced by section 24 of PoFA) provides that, *"The National DNA Database Strategy Board must issue guidance about the destruction of DNA profiles which are, or may be retained under this part of the Act and a chief officer of a police force in England and Wales must act in accordance with guidance issued under subsection (2)."* In January of 2014 the Strategy Board issued Guidance under section 63AB(2) in which it established an 'Early Deletion Process' under which individuals may apply to Chief Constables to have their DNA profiles and/or fingerprints deleted from the national databases before the expiry of the maximum retention periods allowed for under the PoFA regime.

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

249. Updated guidance has been issued in the form of the 'Records Deletion Process' but the situation remains very restrictive[152] and the grounds upon which an individual may apply for deletion of their PNC and biometric records remain unchanged. In the 2015/16 financial year, 233 such deletions where ordered by Chief Officers (see Table 24 below).

250. It is ultimately for Parliament to determine whether these new guidelines give expression to what was intended by section 24 of PoFA.

TABLE 22: Records Deletion Process (Financial Year 2015/2016)

Total Arrests	Total Applications	Approved by Force	Rejected by Force	Rejected as ineligible	Pending
896,209	1,003	233	317	205	208

(Source: ACRO Criminal Records Office[153])

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

[153] *ACRO Criminal Records Office Annual Report 2015-2016* at page 11 (https://www.acro.police.uk/uploadedFiles/Annual%20Report%20A4%202015-16%20spread.pdf)

7. INTERNATIONAL EXCHANGES

7.1 INTERNATIONAL EXCHANGE OF BIOMETRICS

251. One aspect of my oversight role is that of overseeing the sharing of biometric material internationally. The Home Office's International DNA Exchange Policy for the United Kingdom[154] states that:

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

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

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

INTERNATIONAL DATA EXCHANGE POLICIES

253. The international exchange of DNA profiles and associated demographic information is governed by the aforementioned 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.

254. There is no equivalent Home Office policy for the international exchange of fingerprints. This apparent governance deficit has left those agencies responsible for the international exchange of such data to operate without a national government policy steer. This situation is clearly untenable and I will raise this issue again with Home Office officials. It is my hope that now fingerprints have been brought within the remit of the NDNAD&FSB, this further example of discordance between the two types of biometrics will be addressed.

7.2 THE ROLES OF THE UKICB AND ACRO

255. The UK International Crime Bureau (the UKICB) within 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 and European Arrest Warrants and the case management of international enquiries. Except for matters relating to counter-terrorism, most requests for the

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

international exchange of DNA profiles are channelled through the UKICB. The UKICB also deals with the international exchange of fingerprints for intelligence purposes.

256. 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

257. ACRO exchanges criminal conviction data with the other 27 EU member states under Framework Decision 2009/315/JHA. Exchanges take place pursuant to 'Requests' or 'Notifications'.[155] The fingerprints of UK nationals are not sent from the UK to other EU member states in respect of Requests or Notifications.

EXCHANGES WITH NON-EU MEMBER STATES

258. ACRO also exchanges conviction information and fingerprints with non-EU countries on behalf of the NCA and the Home Office. Those exchanges again take place pursuant to Requests and Notifications and may again involve the exchange of fingerprints. The fingerprints of UK nationals are not sent from the UK to other countries in respect of Requests or Notifications.

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

[155] 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

TABLE 23: Fingerprint Exchanges (January-December 2016)

	EU Exchanges	Non-EU Exchanges
Requests in	179	3170
Requests out	36,623	33,047
Notifications in	23	7
Notifications out	20,850	13,520

(Source: ACRO Criminal Records Office)

7.4 EXCHANGE OF DNA AND FINGERPRINTS FOR INTELLIGENCE PURPOSES

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

DNA SAMPLES

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

No DNA samples were exchanged between 01 January 2016 and 31 January 2016.

DNA PROFILES

261. 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 UKICB.[156]

OUTBOUND SUBJECT PROFILES

262. 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 NDNAD Strategy Board and following a full risk assessment.[157]

INBOUND SUBJECT PROFILES

263. DNA subject profiles are received from abroad and sent to the NDU for searching against the NDNAD. The Home Office Policy details the criteria under which searches will be authorised.[158]

OUTBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

264. Unidentified DNA profiles from crime scenes or from unidentified bodies or remains may be sent abroad for searching on another country's DNA database(s) at the request of the police force investigating the crime. The Home Office Policy details the criteria under which DNA profiles will be released from the NDNAD for searching.[159]

INBOUND CRIME SCENE PROFILES AND PROFILES FROM UNIDENTIFIED BODIES

265. DNA crime scene profiles or unidentified body profiles may be received from abroad. The Home Office Policy states that, absent specific authorisation by the NDNAD Strategy Board, the UK will normally only comply with a request for the searching of an inbound crime scene profile if the relevant crime meets the definition of a 'UK Qualifying Offence'.[160] 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*".

---

[156] 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.

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

[158] Ibid at paragraphs 7.1.1.

[159] Ibid at paragraphs 7.2.2.

[160] It seems that, as a general rule, the UKICB will also agree to the searching of an inbound crime scene profile if the relevant offence falls within the ambit of a list of serious offences which has been approved by the Home Secretary.

266. **TABLE 24: DNA Profile Enquiries (January – December 2016)**

	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[161]	4	2	1	139	100	6
Missing Persons	1	1	0	52	26	0
DNA Crime Scene profiles[162]	141	102	10	906	789	30
Unidentified Bodies	10	5	2	69	60	0

(Source: UKICB)

FINGERPRINTS AND FINGER-MARKS

267. There are 4 types of fingerprint enquiry dealt with by the UKICB. In the absence of a national Home Office policy for the international exchange of fingerprints, the UKICB 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 27 below provides the figures for inbound and outbound Fingerprint Requests.

OUTBOUND FINGERPRINTS

268. 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.

[161] (figure includes missing persons)

[162] (figure includes unidentified bodies)

269. Any force which wants fingerprints sent abroad must explain to UKICB why they think that there is a link to the specific country or countries to which the prints are to be sent and must provide a full risk assessment.

INBOUND FINGERPRINTS

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

OUTBOUND CRIME SCENE FINGER-MARKS

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

INBOUND CRIME SCENE FINGERMARKS

272. 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.[163]

TABLE 25: Inbound and Outbound Fingerprint Requests

	Outgoing from UK			Inbound to UK		
Fingerprint Type	**Total**	**Searches Completed**	**Positive/ Potential Match**	**Total**	**Searches Completed**	**Positive/ Potential Match**
Ten-print sets	910	814	Information not available	2346	2328	Information not available
Crime scene finger marks	27	21	Information not available	224	222	Information not available

(Source: UKICB)

[163] However, as with inbound crime scene profiles, it seems that the UKICB 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. See in this regard footnote 160 above.

DIP-SAMPLING

273. My Head of Office has carried out two dip-sampling exercises this year; in May 2016 and January 2017.

274. In May 2016 she dip-sampled 11 cases in which DNA profiles and/or fingerprints had been exchanged internationally. In 2 of the cases DNA searches were conducted for offences which were not listed on the UK qualifying offences list and prior approval had not been sought from the NDNAD Strategy Board as per the Home Office International Exchange Policy. In all of the fingerprint cases sampled, exchanges took place in order to confirm the identity of the subjects involved.

275. During a visit to the offices of the NCA and UKICB in January 2017 my Head of Office dip-sampled a further 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 the NDNAD Strategy Board. These cases had been identified by UKICB through its internal audit processes as not in accordance with the Home Office Policy prior to dip-sampling.

POTENTIAL 'BIOMETRIC BREACHES

276. There have been a number occasions when the UKICB has been proactive in drawing my attention to issues of possible concern as regards the international exchange of biometric material or data. These concerns related to 2 cases where demographic information had accompanied the international exchange of a DNA person profile and 4 cases where incorrect caveats had been sent out with regards to DNA profile retention.

277. Additionally, in the quarterly returns provided to my Office, it has been clear that audit measures have been put in place to identify where searches have been conducted for offences outside of the UK qualifying offences list or otherwise where procedural abnormalities have arisen. Having looked further into these cases, I was satisfied that, although the UKICB had not followed the letter of the Home Office International DNA Exchange Policy, the searches were proportionate given the facts of those cases; however, I have recommended that steps be taken to ensure that police and/or staff are alerted to the procedures that they should follow in future cases.

278. 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.

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

EUROPEAN ARREST WARRANTS

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

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[164] and is responsible for recording all requests received through the SIS II. All EAW requests, whether or not they have a UK connection, are now recorded and this has resulted in a higher number of recorded requests since 2014/15 than in previous years.[165]

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

282. In the fiscal year 2015-16, 241 EAW requests were made by the UK and 14,279 EAW requests were received by it. Table 26 gives a yearly comparison since 2013.

TABLE 26: EAW Requests by fiscal year (2013/14 – 2015/16)[166]

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

[164] '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).

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

[166] See http://www.nationalcrimeagency.gov.uk/publications. Note in this regard the last sentence of paragraph 280.

7.5 INTERNATIONAL CONVICTION INFORMATION

LOADING NON-UK CONVICTIONS TO THE PNC

283. 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;
- 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.[167]

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.[168]

284. 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.

285. Although it was understood that relevant guidance would be finalized 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.

---

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

[168] 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.

UK NATIONALS WHO HAVE OFFENDED ABROAD

286. 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.[169] 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.[170] 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.

7.6 INTERNATIONAL EXCHANGES AND BREXIT

287. Some of the international exchanges explained above depend on EU agreements and 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.

288. The House of Lords[171] when it examined this problem recently concluded:

> "*We welcome the statement by the Secretary of State for Exiting the European Union that "maintaining the strong security co-operation we have with the EU" is one of the Government's top four overarching objectives in the forthcoming negotiations on the UK's exit from, and future relationship with, the European Union. The arrangements currently in place to facilitate police and security cooperation between the United Kingdom and other members of the European Union are mission-critical for the UK's law enforcement agencies. The evidence we have heard over the course of this inquiry points to a real risk that any new arrangements the Government and EU-27 put in place by way of replacement when the UK leaves the EU will be sub-optimal relative to present arrangements, leaving the people of the United Kingdom less safe.*"

289. The House of Lords European Committee Report contains a full summary of the various treaties and arrangements which currently exist with the EU and the possible alternatives. The ongoing uncertainty in this area is undoubtedly worrying some Police & Crime Commissioners since these matters have been raised directly with me.

---

[169] See paragraphs 257-258 of this Report above. 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.

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

[171] *Brexit: future UK–EU security and police cooperatio*n, House of Lords, European Union Committee, 7th Report of Session 2016-17.
http://www.publications.parliament.uk/pa/ld201617/ldselect/ldeucom/77/77.pdf

290. However, not all international exchanges depend on EU arrangements and post-Brexit the UK will remain within broader exchange mechanisms such as Interpol, but these are generally less efficient.

291. 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

292. The Prüm Council Decisions of 2008[172] 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[173], those Decisions were subject to the UK's opt-out under Protocol 36 of the Lisbon Treaty.

293. In December 2015[174] 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 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
- that the operation of the system will be overseen by an independent Prüm Oversight Board.

294. 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[175] database has been agreed by Ministers and I understand that the intention is for exchanges

---

[172] 2008/615/JHA and 2008/616/JHA

[173] (at paragraphs 308-309)

[174] 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.

[175] (Combined DNA Index System)

to 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 by the end of 2017.

295. Whilst it has been made clear by the Government that the Biometrics Commissioner and the Information Commissioner will have seats on the Oversight Board[176] and that they *"will be involved in the process",*[177] the precise nature of my oversight and/or 'auditing' role has yet to be finalised.[178] I shall be concerned to ensure that, since these Prüm exchanges will use an MPS database, proper governance arrangements are in place. Moreover, the overall result is that the operation of international exchanges, at least until the full UK exchange solution is operational, will be split between three policing agencies[179] and begs the question as to whether this is the best arrangement for the future.

---

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

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

[178] See: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 315-317.

[179] The UKICB, MPS and ACRO.

8. FUTURE BIOMETRIC CHALLENGES

8.1 TECHNICAL CHANGE AND NEW CHALLENGES

296. 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 but at the same time there has been a rise in new forms of crime, such as internet-based fraud. Over the same period the risk of internationally inspired terrorist attacks in this country has increased.

297. 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, 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.

298. PoFA only controls the police use of DNA and fingerprints (and footwear impressions) in criminal and national security cases; however, the previous Commissioner's reports drew attention to the development and deployment of other biometric technologies.

299. Last year's Report also 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.[180] At the time of writing, some two years later, the *Review of the Use and Retention of Custody Images* has just been published[181] but the Biometric Strategy is still awaited.

8.2 FACIAL IMAGES

300. The Review of custody facial images was required, at least in part, to respond to a court judgment in 2012[182] which was critical of the governance arrangements then in place and in

---

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

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

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

particular that the retention regime was not proportionate in its treatment of unconvicted persons to the extent that it was unlawful. The Review does propose to extend proportionality by introducing a process by which those not convicted of an offence can apply to the police to have their facial images deleted, but the police have the discretion to refuse such a request. Whether the limited changes proposed will be sufficient in the face of any future legal challenge may depend on the extent to which those individuals without convictions successfully make an application for deletion of their police held custody images. The evidence from a similar application process to the police, to delete PNC and biometric records, is not encouraging.[183] In addition, the proposals are complex and will require a great deal of individual decision making resulting in high compliance costs and, in spite of guidance, may lead to forces exercising their discretion differently thereby resulting in a postcode lottery. I have commented on this matter at greater length elsewhere.[184]

301. The use of facial images by the police has gone far beyond using them for custody purposes. In July 2016 there 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 (and remain) searchable using facial recognition software[185], although it is not clear how many of these are duplicate images or which relate to unconvicted persons. In addition, not all forces are uploading images to PND, including the MPS who hold their own extensive collection, so 19 million is an underestimate. The development of these national PND holdings has been led by the Chief Constable of Durham Police. In addition to these PND holdings, other forces such as Leicestershire and the MPS have also used and stored facial images using different databases and different searching software.

302. Furthermore, the custody and other images stored on the PND and other force systems have been used to try and identify individuals in public places. A recent reported example of this was the Metropolitan Police's use of facial imaging to check those attending the Notting Hill Carnival against a force watch list.

303. My predecessor raised concerns about whether PND was a suitable database for holding such images and about the quality of the image searching software being used and its human interpretation.[186] The main point, however, is that a very rapid growth of the police use of facial images has taken place by different forces using different systems with varying degrees of image quality. Yet, notwithstanding these differences, the recently published

---

[183] See further Records Deletion Process at paragraph 248 of this Report.

[184] See http://www.gov.uk/government/organisations/biometrics-commissioner.

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

[186] See *Commissioner for the Retention and Use of Biometric Material, Annual Report* 2015 at paragraphs 339-344.

Review urges all forces to upload their images to PND. As a recent report by HMIC(S) concluded, *"This means that differing standards are being applied to a common UK database"*.[187] This situation could easily produce differential decision making and potentially runs the risk of false intelligence or wrongful allegations. Such a rapid uncoordinated development and deployment of facial imaging by the police is not unique to the UK.[188] So far there has been little or no public discussion in respect of the retention and use of facial images or whether or how such a regime should be governed. The development has taken place outside the oversight of the NDNAD&FSB which oversees other biometrics, such as DNA and fingerprints.

304. The new Forensic Science Strategy and the Home Office's Biometrics Programme (HOB) provides an opportunity to bring some order and rigour into this somewhat anarchic situation as regards facial images. This process will involve the technical evaluation of alternative storage and image searching software and, equally important, the development of standards in operational use and interpretation. The Forensic Science Regulator has recently drawn attention to these needs.[189] Moreover, this re-development also needs to include consideration of what governance and oversight arrangements for the police use of facial images should be created and whether this should have an independent element.

305. Facial images have been used by the police since the development of photography and in that sense are familiar to us all. However, the development of digital images, their storage on a national database, the use of powerful searching algorithms and the deployment of such technologies in public spaces transforms facial images into something new. Whilst even the best matching algorithms cannot reach the accuracy levels achieved by DNA, and like fingerprints require human interpretation, they are improving and are already being deployed. In addition, unlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge[190] and facial images of about 90% of the adult population already exist in passports or driving licences. Facial images are a powerful new biometric but the acceptance by the public of their use for crime control purposes may depend on the extent to which the governance arrangements provide assurance that their

---

[187] HM Inspectorate of Constabulary in Scotland: *Audit and Assurance Review of Facial Search functionality within the UK Police National Database (PND) by Police Scotland*, January 2016. P7.

[188] Gaines,S and Williams,S: *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown University, Center on Privacy & Technology, 2016

[189] *Forensic Science Regulator, Annual Report 2015-2016* at www.gov.uk/government/publications/forensic-science-regulator-annual-report-2016.

[190] Covert collection of DNA or fingerprints is possible, but much more difficult than the public collection of facial images, and is governed by legislation and subject to stringent independent oversight.

use will be in the public interest and intrusion into individual privacy is controlled and proportionate.

306. Last year's report drew attention to this rapid development in the police's use of facial images and the need to consider technical quality, management, interpretation and governance.[191] The recent Review proposes leaving all these issues solely in the hands of the police without any independent oversight or assurance to reassure the public, especially those individuals whom the 2012 Court judgment[192] described as *"entitled to the presumption of innocence".*[193] It is now almost five years since the Court held that the police retention of facial images was unlawful, yet we still do not have a clear policy in operation to correct that situation.

8.3 OTHER BIOMETRICS

307. Facial images are just the first of a new wave of biometrics. I am aware that the police are already experimenting with voice recognition technology and others such as iris, gait and vein analysis are already commercially available. The use by the police of other biometrics may well be in the public interest and may improve public safety but the points made above in respect of facial images equally apply. Indeed, the lack of clarity about future governance arrangements for new biometrics may actually impede such 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.

8.4 HOME OFFICE PLANS FOR POLICING DATABASES

MANAGEMENT OF DATABASES

308. Until 2007 the Police Information Technology Organisation (PITO) developed and managed IT systems for policing. However, not all police forces used PITO systems, preferring instead to buy their own systems. In 2007 the National Police Improvement Agency (NPIA) came into existence, in part to encourage the development of unified IT systems for policing. NPIA took over the role that PITO had previously played and did achieve some increased unification. In 2012 NPIA was abolished and its functions were transferred to the new National Crime Agency (NCA), or the College of Policing, with the Home Office taking back the IT functions. The Home Office has a work programme to develop and modernise the

[191] (see footnote 186 above)

[192] (see footnote 182 above)

[193] (at paragraph 54 of that judgment)

police IT systems and, in particular, has an ongoing Biometric Programme (HOB) to develop new databases for policing and other government functions.

309. As far as police databases are concerned, the Home Office intends that the NPCC should take over responsibility for developing and owning police IT systems – although I understand that the two main national databases for DNA profiles and fingerprints, as well as PNC and PND will remain under Home Office control. In anticipation the NPCC has re-structured its technical committees to prepare for this new arrangement.[194] Since the NPCC does not have the infrastructure to host national databases directly, these will have to be managed by one or more forces. The police have concerns as to whether such transfers will also come with the current resource attached to them. If central funding does not continue, then, the police service collectively will have to find some way of funding the forces that host national databases.

DNA & FINGERPRINTS DATABASES: QUALITY AND GOVERNANCE.

310. The new arrangements for databases are not a matter for me, except for the fact that at present the national DNA and fingerprint databases are managed by the Home Office and overseen by the National DNA Database & Fingerprint Database Strategy Board (NDNAD&FSB). The Strategy Board has assured the quality of the data and its use and, since it is chaired by a representative of the NPCC, it can issue guidance to police forces on PoFA compliance and re-engineer the databases to support compliance.

311. What this means is that there is a mechanism (the NDNAD&FSB) to provide both oversight of data quality and governance of these two databases. As long as the databases remain within the Home Office and the NDNAD&FSB continues then this will remain the case. Neither facial images (nor other biometrics) are covered by PoFA or overseen by the NDNAD&FSB.

FOOTWEAR IMPRESSIONS

312. There are two national databases of footwear impressions.[195] The retention of this data, as for DNA and fingerprints, is governed by PoFA.[196] At present the databases are managed by the Home Office[197] but I understand that the intention is that they should be transferred to West Yorkshire Police to manage on behalf of the NPCC. It is not clear whether West

---

[194] By creating a new Information Management & Operational Requirements Coordination Committee (IMORCC) to oversee future developments.

[195] See paragraphs 47-52 of this Report above.

[196] (see section 15 of PoFA)

[197] The NDNAD NDU currently performs this function.

Yorkshire Police will also be responsible for ensuring the quality of the data and providing the governance for its use or whether this will be provided directly by the NPCC. Nor is it clear how the costs of managing the database will be met or even if West Yorkshire will accept responsibility for managing the database.

313. Since footwear impressions are included in my remit this uncertainty may affect PoFA compliance or, if needed, the development of national guidance.

GOVERNANCE OF DATABASES

314. At present we are in a period of transition and it is not clear how oversight and governance for other biometrics databases will be provided and what the role of the Home Office and the NPCC will be. The HOB Programme is developing replacement biometric databases apace but is not developing quality or governance processes in parallel. Furthermore, the new biometric databases will host DNA, fingerprints and facial images[198] and potentially future biometrics. The first two are covered by PoFA and overseen by the NDNAD&FSB but the latter by neither.

315. During this period of transition, a unified national approach exists in some cases but not in others. Even in the case of DNA and fingerprints, previous Reports have identified examples of a disjointed approach to PoFA compliance and the present report discusses how these are being dealt with. The lack of a unified approach could lead to missed opportunities for the successful criminal justice use of biometrics to protect the public or, equally, it could lead to the production and use of poor quality data, flawed application processes and unintended consequences.

316. Uncertainty during a period of transition is understandable but in this case is a result of a lack of clarity, beyond the general transfer of ownership to the NPCC, about how biometric data quality and governance in general will be provided in the future. The police service is aware that its future control and use of databases needs to be accepted as legitimate by the public and that clear governance, probably with an independent element and a clear legislative framework, may be necessary to achieve that end.

8.5 BIOMETRIC USE ASSURANCE

317. Any biometric used for policing will have the common characteristics of a 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

[198] The databases will not host new datasets, but will replace the existing databases.

technologies work operationally will depend on the quality of the data collected, how the matching algorithm works and its quality, 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 use of biometrics. Failure to control and manage 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.[199]

318. For all biometric use by the police the public will expect that mechanisms exist to prevent, or at least minimise, the risk of such a failure. Assurance is more likely to be publicly accepted as credible if it is transparent and also has a degree of independence. If a biometric is to be used in evidence as part of a prosecution, transparency of the system and the technology and processes that underpins the claimed match is evidentially essential.

319. For fingerprints and DNA such assurance is currently provided by the combination of the Forensic Science Regulator, overseeing scientific quality and interpretation; the NDNAD&FSB, overseeing database management and use; and my Office, overseeing governance and legislative compliance. However, some of the emerging biometrics will be more complicated to assure. Some commercially available biometric software now uses machine learning or neural networks to improve analytic ability but, by doing so, it can be difficult, if not impossible, to understand how that software is determining possible matches. This is 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.[200] This scientific problem raises issues for ethics and governance since transparency, and therefore accountability, can be difficult if not impossible to achieve. The 'Black Box Problem' also raises the practical issue of what reliance can be placed on such systems in judicial decision making. There have already been examples of biases emerging in such systems. This problem is not unique to biometric systems but the police use of biometrics in a criminal justice context make it particularly acute.[201]

---

[199] The same point has recently also been made by the Forensic Science Regulator – see *Forensic Science Regulator: Annual Report 2015-16.*

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

[201] 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.

8.6 TRANSFORMATIVE DATA USE

320. The use of biometrics is just one example of the very significant police use of data that is gathering pace. The Home Office has a development programme (HOB) to update the systems behind the retention and use of biometrics, but alongside this another aspect of the programme is working to develop the broader use of data and analytics. These strands will transform the nature of policing to the extent that the College of Policing has recognised that this will require police officers with different skill sets and has consequently launched a new Policing Education Qualifications Framework (PEQF) to address this issue.[202]

321. All of us leave records of our activities across public and private databases and in public spaces which, if analysed holistically, provide multiple ways of checking identity, modeling the patterns of our social behaviour, collecting or inferring our attitudes and recording our activities, movements and decisions. Therefore to biometrics we should now add sociometrics.[203] We are already accustomed to simple versions of such analytics, for example when websites offer us goods or services tailored to predictions of our preferences or needs.

8.7 FUTURE STATE USE OF DATA

322. The ranges of data which the state holds are large and so potentially can be used by these powerful analytic techniques. Such use of 'big data' is still in its infancy and the analytic techniques needed are by no means easy but they are being developed rapidly. The Home Office's plans initially involve data sharing between the Home Office family of agencies, for example by sharing facial images between policing and border control. However, sharing with other government agencies is already developing, for example in the case of facial images with DVLA and the prison service. In addition, private agencies are developing similar abilities and sometimes piggy-backing on government systems.[204]

323. My intention in raising these points[205] is not to raise a scare about future data use; there are significant potential public benefits from such developments, if only to improve the

---

[202] See: http://www.college.police.uk/News/College-news/Pages/PEQF_media_launch_blog.aspx

[203] 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.

[204] The government 'Verify' programme allows commercial companies to authenticate identity in order to allow access to government systems, with the government setting the standards. Verify may also be used by the private sector for non-government authentication purposes (http://www.Gov.UK/Verify).

[205] (at sections 8.5-8.7 of this Report)

efficiency of the delivery of public services.[206] At the same time 'big data' will change the relationship between the citizen and the state in a country that has sometimes thought of freedom as having a civil realm over which the state has minimal knowledge or control; that privacy and liberty are conjoined. As in the specific case of facial images discussed above, these developments have been the subject of little public or Parliamentary scrutiny and it is unclear under what governance arrangements they will operate.

8.8 LESSONS FROM POFA

324. As the current Biometrics Commissioner my role is defined and limited by PoFA. Notwithstanding this, having overseen the PoFA arrangements, there are some lessons that government and Parliament may wish to consider as regards the future development of these new biometrics and data analytics.

i) The future direction of travel will need to command public confidence to be seen as legitimate.

ii) The public need assurance that the use of data by the state will properly balance the public interest against the individual's right to privacy (proportionality).

iii) Clear governance arrangements are necessary to provide that assurance.

iv) A legislative framework and independent oversight provides transparency of governance and assurance to Parliament and the public and helps to build public confidence and therefore legitimacy.

v) Increasingly governance will need to operate at a pan-government level as data is shared across government departments and agencies.

vi) Governance will need to consider non-state actors use of data and links between the public and private sectors.

vii) The difficult judgment as to the proper balance between public and private interest (proportionality) is best taken by Parliament expressed through legislation and not left to the agency using the data (such as the police).

viii) Parliament decided on a combination of bright-line rules and discretionary decision-making in order to ensure the proportionality of the retention and use of DNA and

[206] See eg: Drew, C: *Data ethics in government*, Philosophical; Transactions of the Royal Society A, November, 2016

fingerprints in the PoFA regime but at the cost of complexity which has increased compliance costs.

ix) The costs and burden of regulation can be minimised by legislation that takes account of the operational context and above all by parsimony and simplicity.

x) The proportionality of biometric and other data use and retention rules needs to be consistent across different types of data.

xi) Multiple systems of biometric (or data) governance will increase compliance costs and run the danger of confusing both those operationally responsible and the public.

xii) The specific case of regulation of the police use of biometrics has to be considered in the context of the police general use of data and the broader state use of data.

9. OFFICE OF THE BIOMETRICS COMMISSIONER AND BUDGET

9.1 OFFICE OF THE COMMISSIONER

325. The Office of the Biometrics Commissioner is independent of government and has a staffing compliment of four staff who are civil servants seconded from the Home Office's Office of Security and Counter-Terrorism (OSCT). Due to various reasons touched upon in previous Annual Reports the Commissioner's Office has been understaffed. This reduction in resources has impacted on the extent of the work the Office has been able to undertake.

9.2 BUDGET

326. The present budget for the Office of the Commissioner for 2016/7 is £302,000. 80% of the budget is ring-fenced for staffing and previous under-spends in the budget have been entirely due to the under-staffing of the Office.

APPENDIX A

ADDITIONAL NATIONAL DNA DATABASE DATA

NDNAD HOLDINGS

TABLE A01: Profiles retained on the NDNAD by Chemistry Type (year ending 31 December 2016)

Chemistry type	Subject Profile	Crime Scene Profile
SGM	307,485	3,934
SGM+	5,010,878	454,148
DNA-17	533,293	85,270

SEARCHES

1. Each time a subject Profile or Crime Scene profile is loaded to the NDNAD it is searched against existing holdings. While a profile is held on the NDNAD it is constantly searched each time a new profile is added.

2. There are a number of situations where it would not be appropriate to load a DNA profile to the NDNAD, for example if a foreign sample is received for searching. In such cases, it is possible to perform a one-off speculative search against the NDNAD (See Table A02 below).

TABLE A02: One-off Speculative Searches against the NDNAD (January-December 2016)

	UK Searches	International
Total	**5,345**	**934**
Positive	2,905 (54%)	28 (3%)
Negative	2,440 (46%)	906 (97%)

As is evident from Table A02, the vast majority of international searches provide a negative result.

APPENDIX B

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[207]

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.

[207] 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.

   In this context a 'recordable offence' is, broadly speaking, any offence which is punishable with imprisonment[208] 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.[209]

6. 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 43 of the main Report above.

INDIVIDUALS ARRESTED FOR QUALIFYING OFFENCES

7. A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.[210]

8. 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.

---

[208] See section 118 of PACE

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

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

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).

INDIVIDUALS UNDER THE AGE OF 18 YEARS

9. 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.[211]

- 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

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

10. 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.[212] 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 E**).

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

11. 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[213], the resulting 3 year retention period may be extended for a further

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

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

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

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.

12. Sections 63F(7) to (10) of PACE provides as follows.

> *"(7) The responsible chief officer of police or a specified chief officer of police may apply to a District Judge (Magistrates' Courts) for an order extending the retention period.*
>
> *(8) An application for an order under subsection (7) must be made within the period of 3 months ending on the last day of the retention period.*
>
> *(9) An order under subsection (7) may extend the retention period by a period which—*
>
> *(a) begins with the end of the retention period, and*
> *(b) ends with the end of the period of 2 years beginning with the end of the retention period.*
>
> *(10) The following persons may appeal to the Crown Court against an order under subsection (7), or a refusal to make such an order—*
>
> *(a) the responsible chief officer of police;*
> *(b) a specified chief officer of police;*
> *(c) the person from whom the material was taken."*

CONVICTIONS OUTSIDE ENGLAND AND WALES

13. By sections 61(6D), 62(2A) and 63(3E) of PACE[214] the police have, with the authority of an officer of the rank of inspector or above, power to take fingerprints and a DNA sample from (broadly speaking) any person who has been convicted outside England and Wales of an offence that would constitute a qualifying offence under the law of England and Wales. By section 63J of PACE[215] the police have the power to retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample. 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.

14. 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

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

[215] (inserted by section 6 PoFA)

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.

15. EU Council Framework Decisions[216] detail the mechanisms for the exchange and use of foreign conviction information by EU member states. Where a UK national is convicted in another member state, the relevant UK authorities will be notified of that fact and, if the offence is a recordable offence, the conviction will be recorded on the PNC.

16. As regards the nationals of other member states who are present in the UK, as a general rule, information about foreign convictions which is obtained in response to a request such as is referred to above is not, and cannot be, recorded on the PNC. However, in January of 2010 the Home Secretary approved a list of offences in relation to which an exception should be made to that general rule.[217] That list was approved on the basis that individuals who had committed those offences would represent "an immediate and serious threat to public security". Although those offences ('the listed offences') include a number of the more serious 'qualifying' offences, they by no means include all such offences.

[216] 2009/315/JHA and 2009/316/JHA

[217] This list was subsequently updated and amended in 2014.

APPENDIX C

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.[218] Whereas a Chief Officer may only make an application under section 63G(3) if they consider that the retention of the material "*is necessary to assist in the prevention or detection of crime"*, section 63G(2) imposes no express requirement that there be some anticipated public interest in the retention of the material.

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

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

v. Although it is provided at sections 63G(5) and (6) that the person to whom the material relates must be informed of any application for extended retention and given the opportunity to make representations against it[219], 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"*.

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.]

---

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

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

CORE PRINCIPLES AND RELEVANT FACTORS

5. The Commissioner's approach 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.[220] The Strategy Board has endorsed the Commissioner's approach as regards such applications and the detailed Guidance document which it issued in September 2013 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[221], 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.[222]

---

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

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

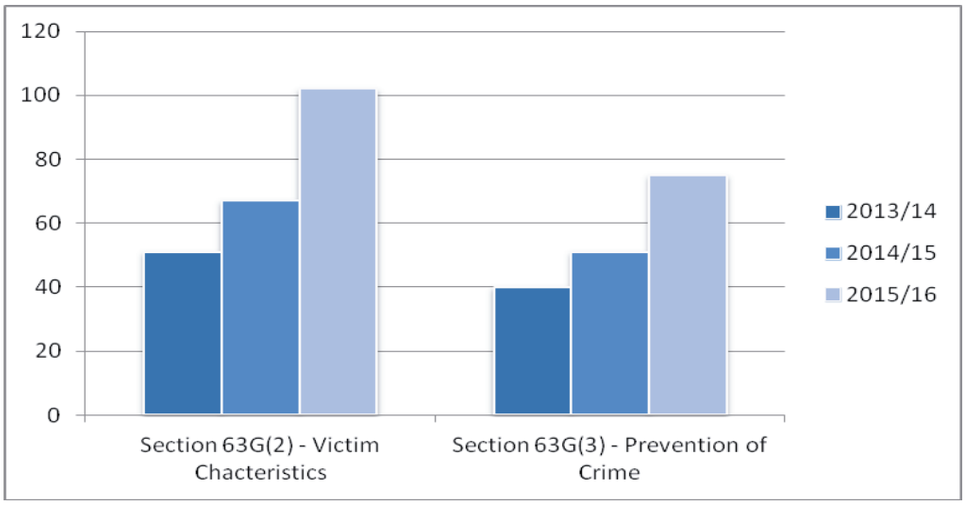
[222] See further Appendix A: Applications to District Judges (Magistrates Court)

APPENDIX D

STATISTICS ON APPLICATIONS TO THE COMMISSIONER TO RETAIN BIOMETRICS

STATUTORY BASIS FOR APPLICATIONS TO THE COMMISSIONER

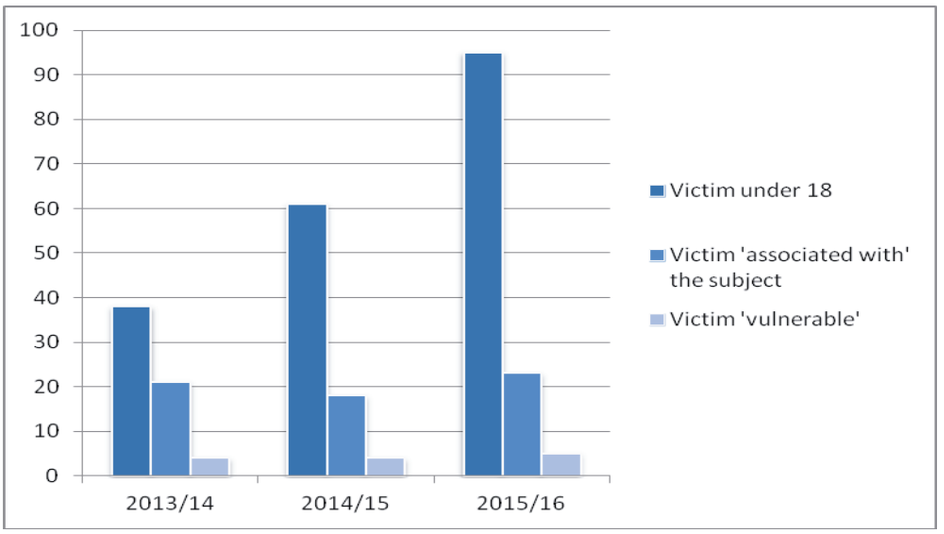
Figure D01: Statutory Basis for Applications to the Commissioner



Statutory Basis for Applications	2013/14	2014/15	2015/16
Section 63G(2) - Victim Characteristics	51	67	102
Section 63G(3) - Prevention of Crime	40	51	75

The distribution between the statutory bases for applications has remained similar between 2013 and 2016.

Figure D02: Applications Under Section 63G(2) – Victim Characteristics

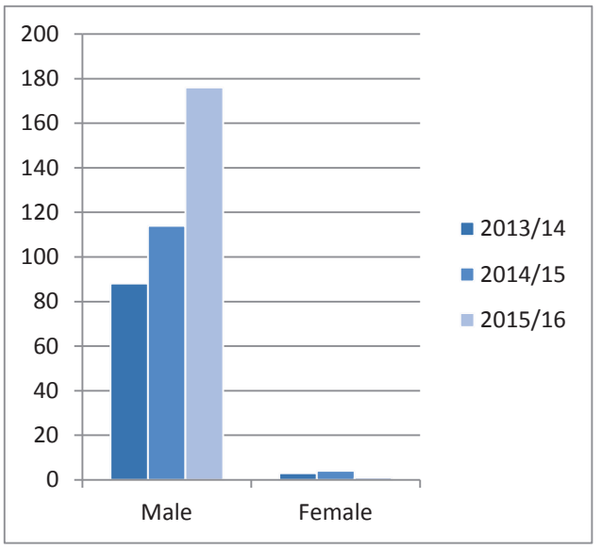


Section 63G(2) applications	2013/14	2014/15	2015/16
Victim under 18	38	61	95
Victim 'associated with' the subject	21	18	23
Victim 'vulnerable'	4	4	5

Since more than one victim characteristic can apply comparisons must be treated with caution but there has been a significant increase in applications where the victim was under 18.

APPLICATIONS: SUBJECT CHARACTERISTICS

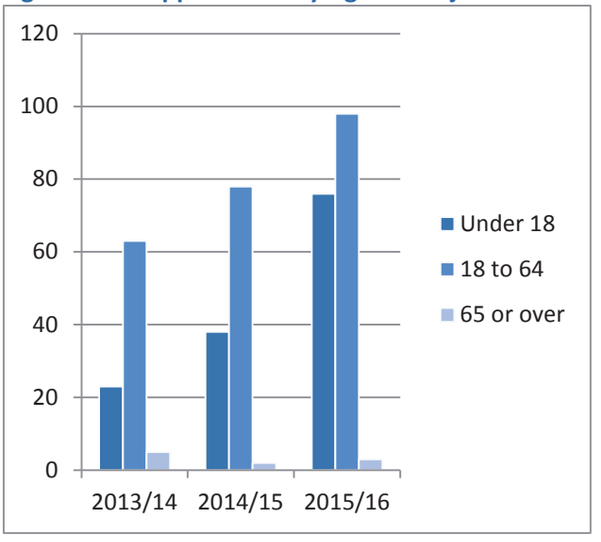
Figure D03: Applications by Gender of Subject



Gender	2013/14	2014/15	2015/16
Male	88	114	176
Female	3	4	1

Predominantly applications have been made in respect of male subjects.

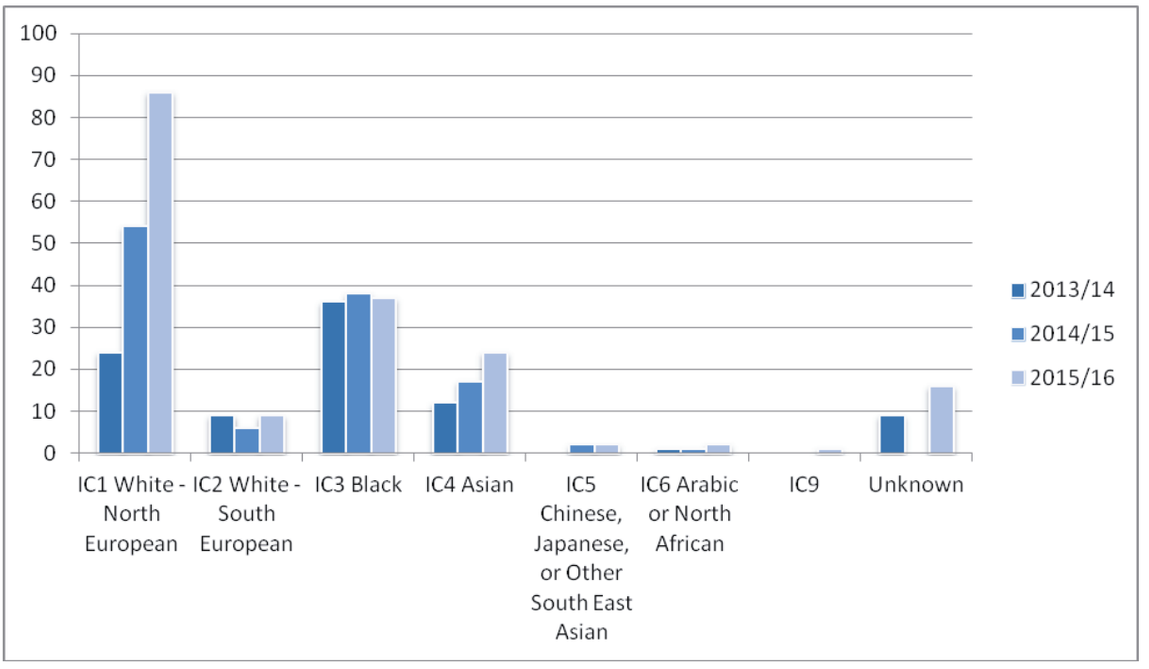
Figure D0 4: Applications by Age of Subject



Age	2013/14	2014/15	2015/16
Under 18	23	38	76
18 to 64	63	78	98
65 or over	5	2	3

As in Fig.2 there has been an increase in the proportion of applications where subjects have been under the age of 18 at the time of the alleged offence.

Figure D05: Applications by Ethnicity of Subject

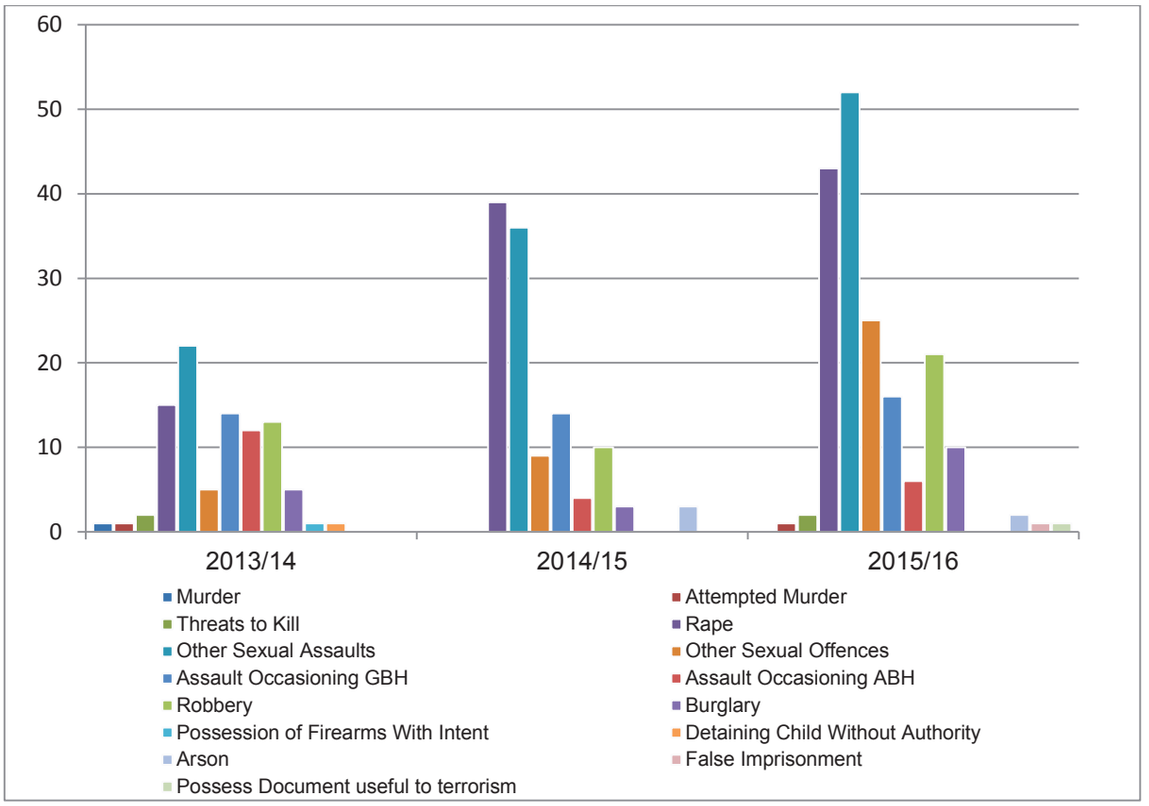


Ethnicity	2013/14	2014/15	2015/16
IC1 White - North European	24	54	86
IC2 White - South European	9	6	9
IC3 Black	36	38	37
IC4 Asian	12	17	24
IC5 Chinese, Japanese, or Other South East Asian	0	2	2
IC6 Arabic or North African	1	1	2
IC9	0	0	1
Unknown	9	0	16

Both black and Asian ethnic groups appear to be over-represented relative to the population but this may reflect the police force areas where applications are coming from and the kinds of crimes involved.

APPLICATIONS: QUALIFYING OFFENCES

Figure D06: Applications by Qualifying Offence



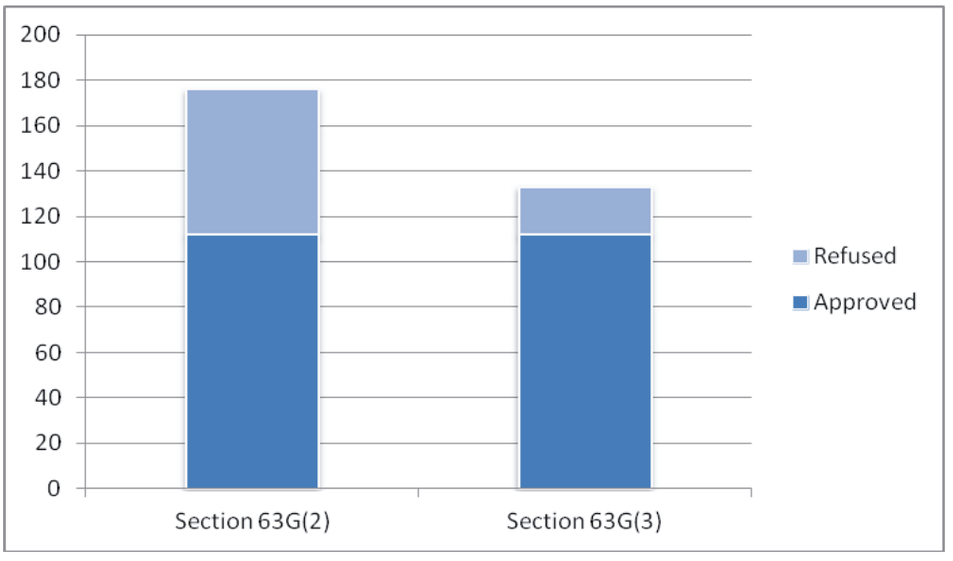
Offence	2013/14	2014/15	2015/16
Murder	1	0	0
Attempted Murder	1	0	1
Threats to Kill	2	0	2
Rape	15	39	43
Other Sexual Assaults	22	36	52
Other Sexual Offences	5	9	25
Assault Occasioning GBH	14	14	16
Assault Occasioning ABH	12	4	6
Robbery	13	10	21
Burglary	5	3	10
Possession of Firearms With Intent	1	0	0
Detaining Child Without Authority	1	0	0
Arson	0	3	2
False Imprisonment	0	0	1
Possess Document useful to terrorism	0	0	1

Sexual offences, taken together, now make up more than half of all applications to the Biometrics Commissioner.

STATISTICS ON OUTCOMES OF APPLICATIONS TO THE COMMISSIONER

APPLICATION OUTCOMES: STATUTORY BASIS

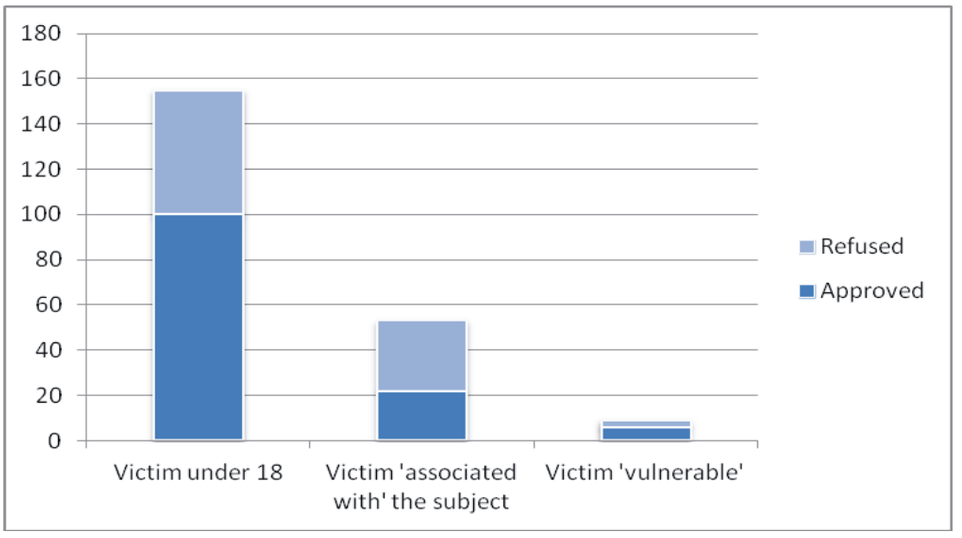
Figure D07: Section 63G(2) Application Outcomes by Victim Characteristics (31 October 2013 – 31 December 2016)



Statutory Basis for Applications	Approved	Refused	Total
Section 63G(2) - Victim Characteristics	112	64	176
Section 63G(3) - Prevention of Crime	113	21	133

APPLICATIONS OUTCOMES: VICTIM CHARACTERISTICS

Figure D08: Section 63G(2) Application Outcomes by Victim Characteristics (31 October 2013 – 31 December 2016)

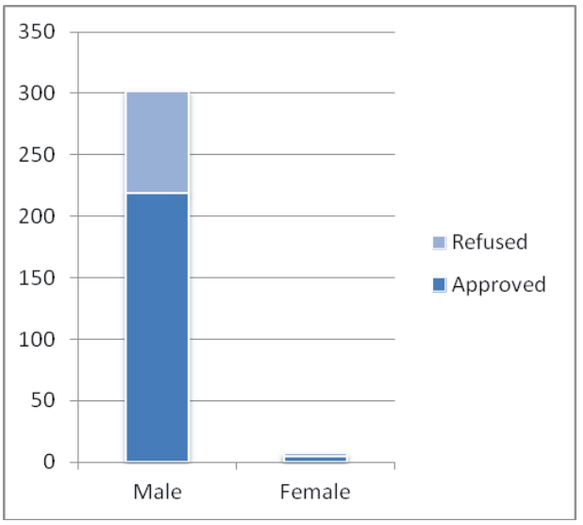


Outcome	Victim under 18	Victim 'associated with' the subject	Victim 'vulnerable'
Approved	100	22	6
Refused	55	31	3

The numbers represented are as yet too small to draw any meaningful conclusions.

APPLICATION OUTCOMES: SUBJECT CHARACTERISTICS

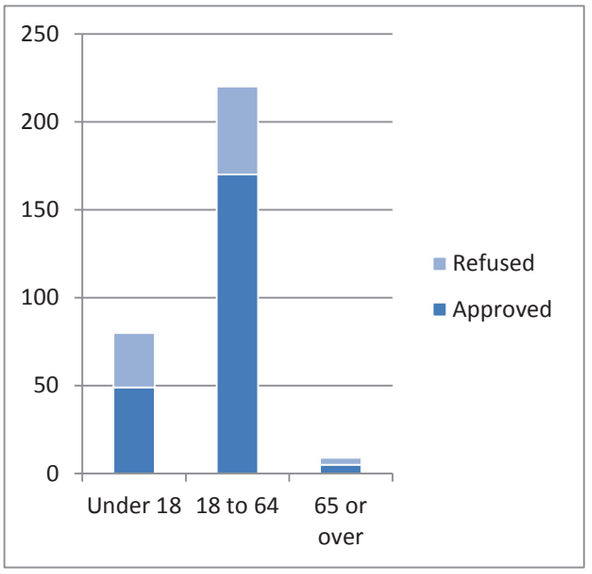
Figure D09: Application Outcome by Gender of Subject (31 October 2013 – 31 December 2016)



Outcome	Male	Female	Total
Approved	219	5	224
Refused	83	2	85
Total	**302**	**7**	**309**

The numbers for females are too small to make meaningful comparisons.

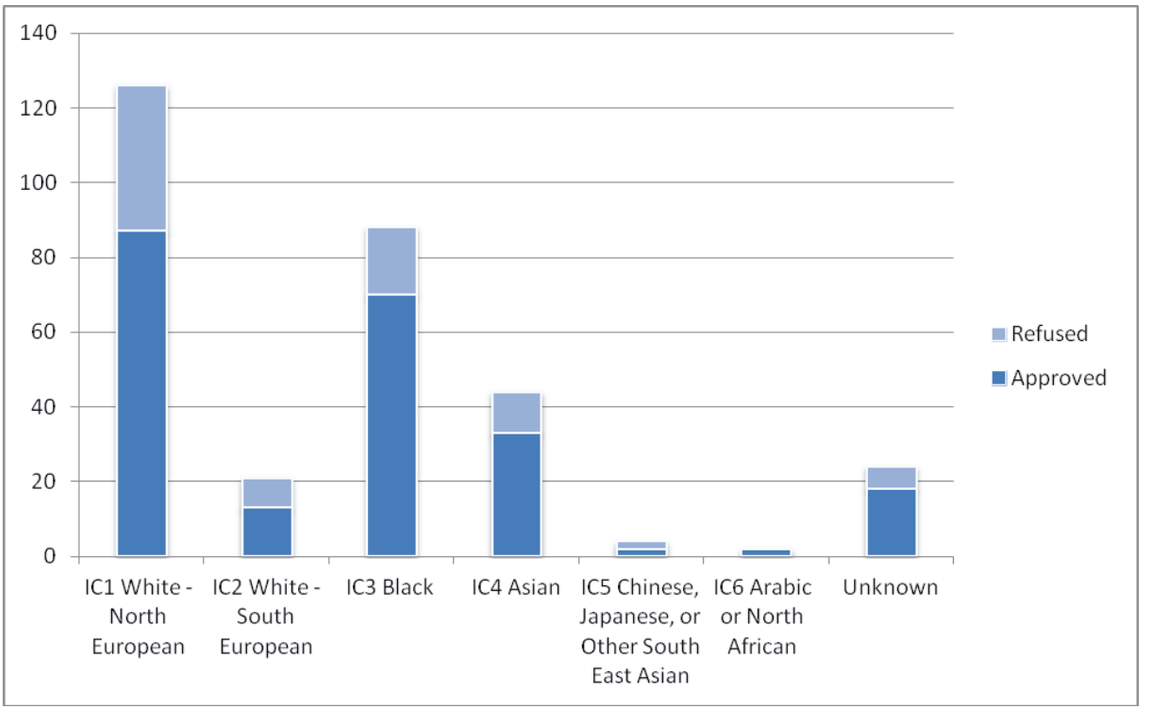
Figure D10: Application Outcome by Age of Subject (31 October 2013 – 31 December 2016)



Outcome	Approved	Refused	Total
Under 18	49	31	80
18 to 64	170	50	220
65 or over	5	4	9
Total	**224**	**85**	**309**

The numbers are very small for the 65+ age group but there is a suggestion of a higher refusal rate for subjects under 18 years.

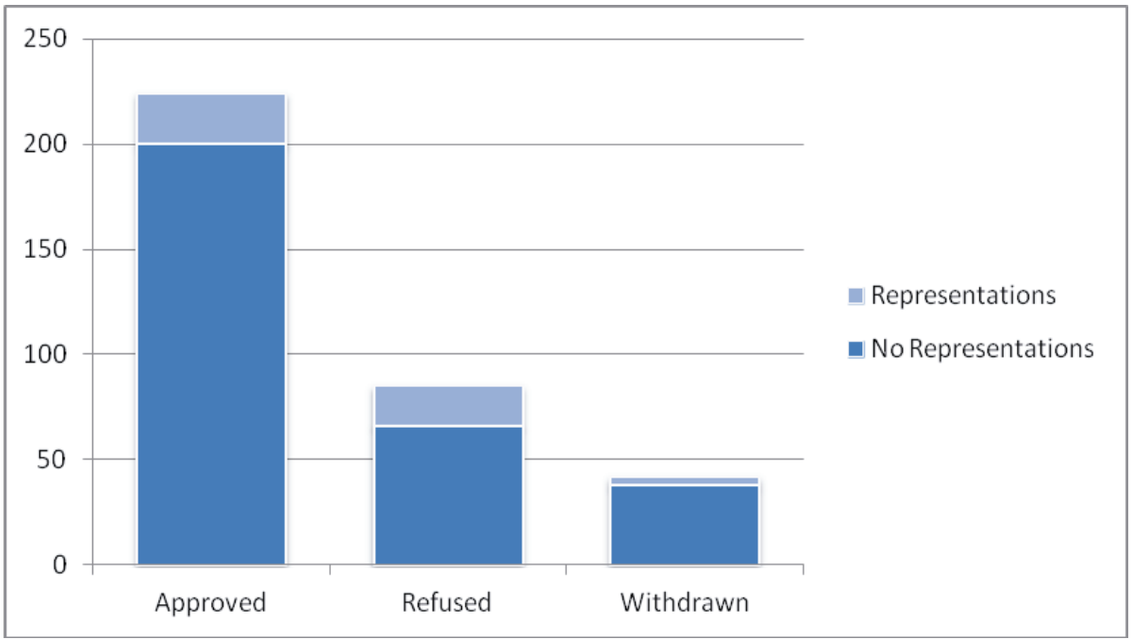
Figure D11: Application Outcome by Ethnicity of Subject



Ethnic Group	Approved	Refused	Total
IC1 White - North European	87	39	126
IC2 White - South European	13	8	21
IC3 Black	70	18	88
IC4 Asian	33	11	44
IC5 Chinese, Japanese, or Other South East Asian	2	2	4
IC6 Arabic or North African	2	0	2
Unknown	18	6	24
Total	**225**	**84**	**309**

APPLICATION OUTCOMES: REPRESENTATIONS

Figure D12: Application Outcomes – Representations made by Subjects (31 October 2013 – 31 December 2016)

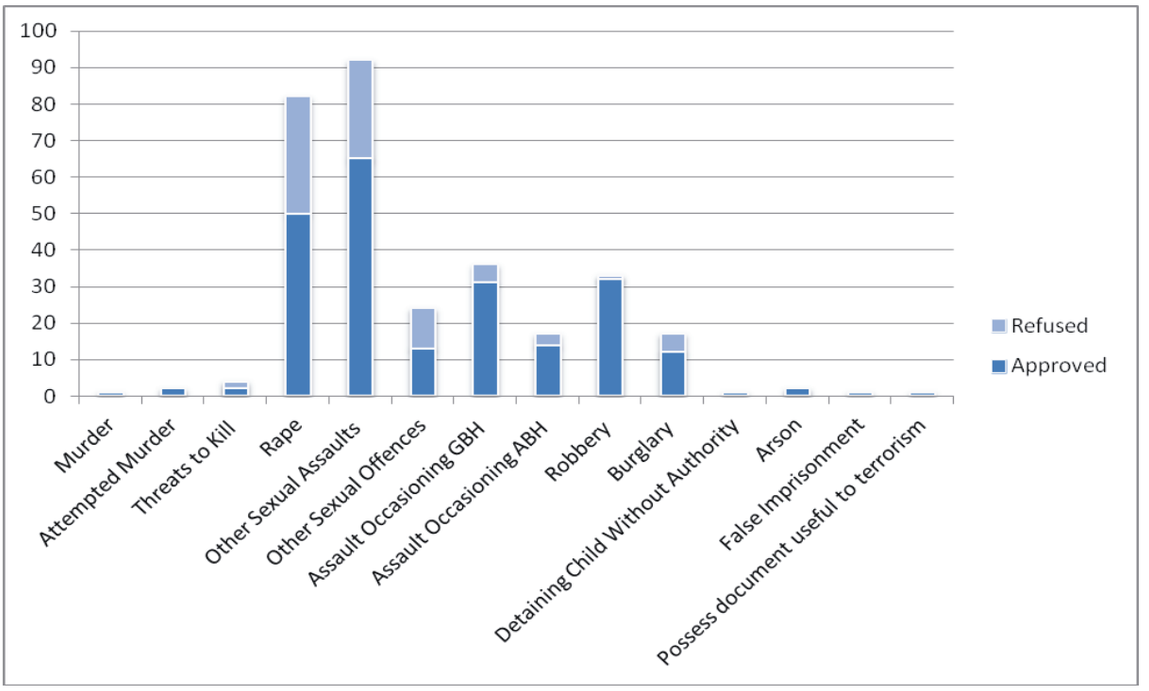


Outcome	No Representations	Representations
Approved	200	24
Refused	66	19
Withdrawn	38	4

Again the numbers represented are too small to draw meaningful conclusions and any differences may be an artefact of the selection of cases for which applications are made.

APPLICATION OUTCOMES QUALIFYING OFFENCES

Figure D13: Application Outcomes by Qualifying Offence (31 October 2013 – 31 December 2016)



Offence	Total	Approved	Refused
Murder	1	1	0
Attempted Murder	2	2	0
Threats to Kill	4	2	2
Rape	82	50	32
Other Sexual Assaults	92	65	27
Other Sexual Offences	24	13	11
Assault Occasioning GBH	198	31	5
Assault Occasioning ABH	17	14	3
Robbery	33	32	1
Burglary	17	12	5
Detaining Child Without Authority	1	1	0
Arson	2	2	0
False Imprisonment	1	1	0
Possess document useful to terrorism	1	1	0
Total	**313**	**227**	**86**

The numbers are small but there is a suggestion that the refusal rate for sexual offences is generally higher than for other offences.

APPENDIX E

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'.[223]

4. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[224] 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,[225] in practice the same 2-year maximum is applied. An NSD may be renewed before its expiry for a further period of 2 years.

---

[223] 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.

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

[225] (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.[226] 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

---

[226] (see footnote 224 above).

- if on reviewing an NSD the Commissioner concludes that it is not necessary for any material retained pursuant to the determination to be so retained, the Commissioner may order the destruction of the material if it is not otherwise capable of being lawfully retained.

STATUTORY GUIDANCE

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.
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 JFIT 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."* [227]

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

13. 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:

---

[227] 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."*

"45. The Chief Officer or Constable must carefully consider all relevant evidence in order to assess whether there are reasonable grounds for believing that retention is necessary for the purpose of national security. In doing so, they may wish to consider any or all of the following non-exhaustive categories of information:

a) Police intelligence

b) Arrest history

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

d) International intelligence

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

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

14. 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.

15. 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

16. 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.

17. 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. It is therefore necessary to specifically ask JFIT to grant access to that information and documentation in cases where the Commissioner wants to see it.

COMMISSIONER'S REVIEW PROCESS

18. 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.

19. Although the Commisisoner'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.*"

20. 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.[228]

21. 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.

---

[228] 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.

(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

- 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.

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

22. 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

23. 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).

24. 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[229] the police and relevant law enforcement agencies were given two years (i.e. until 31 October 2015) to assess that material and to decide whether or not to apply for NSDs in relation to it. In practice, then, since 31 October 2013 Legacy Material which cannot otherwise lawfully be retained has been subject to a maximum retention period of 2 years unless an NSD is made in respect of it. If an NSD is made in relation to such Legacy Material before 31 October 2015, that material may be retained for the period that that NSD has effect.

25. 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:

[229] 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)

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

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

27. 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

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

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
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
NDNAD&FSB	National DNA Database and Fingerprint Databases Strategy Board
NDU	NDNAD Delivery Unit
NFA	No Further Action
NPCC	National Police Chiefs' Council (formerly known as the Association of Chief Police Officers ('ACPO')
NSD	National Security Determination
OBC	Office of the Biometrics Commissioner
PACE	Police and Criminal Evidence Act 1984
PIFE	Police Immigration Fingerprint Exchange
PNC	Police National Computer
PND (*a* or *the*)	*A* Penalty Notice for Disorder or *the* Police National Database
PoFA	Protection of Freedoms Act 2012
PSNI	Police Service of Northern Ireland
SOFS	Secure Operations – Forensic Services (formerly known as Counter Terrorism Forensic Services ('CTFS')
SPOC	Single Point of Contact
TACT	Terrorism Act 2000
TPIMs Act	Terrorism Prevention and Investigation Measures Act 2011
UKAS	United Kingdom Accreditation Service
UKICB	United Kingdom International Crime Bureau

CCS0917991760
ISBN 978-1-5286-0032-3