Annual Report 2018

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Paul Wiles

March 2019

Office of the Biometrics Commissioner

ANNUAL REPORT 2018

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

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

June 2019

This publication is available at www.gov.uk/official-documents

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

ISBN 978-1-5286-1551-8
CCS0319869991 06/19

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

Office of the Biometrics Commissioner

The Rt. Hon. Sajid Javid, MP
Secretary of State for the Home Department
Home Office
2 Marsham Street
London

29th March 2019

Dear Home Secretary,

On 1st June 2016 I was appointed under section 20(1) of the Protection of Freedoms Act 2012 as Commissioner for the Retention and Use of Biometric Material.

By section 21 of that Act I must make a report to you about the carrying out of my functions including my oversight of the police taking, retention and use of DNA and fingerprints. In addition, I must report on the making of National Security Determinations by Chief Officers of Police and the use to which the biometric material held under those determinations is being put. I must also report on the exercise of my powers when the police apply to me under section 63G of PACE 1984 (as amended by PoFA) to retain the biometrics of someone arrested for a qualifying offence but not charged or convicted.

I attach my report covering the year 2018 which provides the above information. This is my third Annual Report as Commissioner for the Retention and Use of Biometric Material.

On receiving my report, you are obliged to publish it and to lay a copy of the published report before Parliament. You may, however, exclude from publication any part of the report if, in your opinion (and after consultation with me) the publication of that part would be contrary to the public interest or prejudicial to national security. There is no Confidential Annex to this report and my hope is that you will feel able to lay it before Parliament in its entirety.

I am happy to discuss the report with you or your Ministers before you lay the report before Parliament.

Yours sincerely,

Paul Wiles
Commissioner for the Retention and Use of Biometric Material

FOREWORD

This is the fifth 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 29th March 2019.

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) since these were discussed in detail in previous Reports and especially in the first two Annual Reports, all of which are available on the Commissioner's website.[1]

My Office should consist of four staff to help deal with my casework functions and the programme of inspection visits and meeting attendance necessary for writing this Report. Until this year I did not have four staff and producing a report for the Home Secretary was only possible by allowing other work to fall behind. This year things have changed and my new Head of Office, Lucy Bradshaw-Murrow, by dedicated effort managed the appointment of three additional staff. Initially, most of the time of these new colleagues had to be spent on catching up with the casework backlog that had built up and this has now been done. What full staffing did allow was for us to complete many more visits to Police Forces this year than in the past and we have visited over half the Forces in England and Wales. We have also been able to participate in more discussions about PoFA related issues both inside and outside government and to engage with the Scottish Government's proposal for new legislation governing the police use of present and future biometrics.

I owe my especial thanks to Lucy Bradshaw-Murrow who, whilst new to post, appointed new staff, trained them and dealt with the casework backlog and also undertook the police force visits. To my new colleagues, Tahmida Hussain, Jalal Ahmed and Kamran Ali, I am grateful for all their hard work and support during the year. To all my colleagues I owe a very real debt of gratitude for their professionalism and unfailing good humour despite the pressures they had to cope with. I also owe thanks to the many police officers and civilian staff of all ranks and civil servants across government but especially in the Home Office who dealt with my incessant demands with unfailing good humour and courtesy.

This year I have discussed at greater length the need for new legislation to allow for the development of new biometrics by the police. In normal times this might have been subject to more public and Parliamentary discussion than has been the case and I might not have devoted so much space to the topic. Whilst such discussion has been happening in Scotland the all dominating Brexit focus of Westminster has marginalised this among many other issues.

Paul Wiles
March 2019

1 https://www.gov.uk/government/organisations/biometrics-commissioner

CONTENTS

SUMMARY

After an introductory chapter on the work of the Biometrics Commissioner, Chapter 2 discusses the gap between the pace of technical developments in biometrics and machine learning, and the ability of governments to respond.

CHAPTER 2: THE CHALLENGE OF NEW BIOMETRICS

The last year has seen the rapid technical improvement of a range of new biometrics. A consistent theme has been the difficulty that legislators have keeping up with the pace and implications of these developments, and the challenge of framing legislation that will remain viable in the face of constant technical change.

This has raised a number of issues. First, should the police use of new biometrics be regulated in a similar way to their use of fingerprints and DNA through legislation? Secondly, should the police conduct of experimental trials with the new technologies be guided in such a way as to provide the comparative knowledge base that will be needed for the operational choices that the police will have to make between the available biometrics? Thirdly, should clearer rules be put in place to regulate inter-governmental access to the new databases that government is developing, and should they have legislative force? Fourthly, should the police development of machine learning based analytics be regulated in the same way as biometrics, since if they involve behavioural data they are 'biometrics' as defined by both data protection legislation and the Home Office's Biometrics Strategy?

CHAPTER 3: CHANGES IN POLICING AND UNINTENDED CONSEQUENCES

The main issues that have arisen this year in relation to the police use of fingerprints and DNA have been the unintended consequences of other changes in policing. The two most important of these have been the increased use by the police of voluntary attendance instead of arrest and the changes made to the police use of bail. The overall result has been a decline in the number of new suspect DNA profiles and fingerprints being added to the national DNA and fingerprint databases, which will lead to a long-term decline in the utility of police biometrics. A less significant but continuing issue has been the tension between the requirement under PoFA to destroy DNA samples after a short period and the requirement of other legislation to retain such samples in some circumstances.

A general theme behind these issues has been the inability of the Home Office to predict the consequences of its actions. Further, the problems that have arisen have been exacerbated by the fact that neither the Home Office and nor the police service have promptly provided practical guidance to mitigate these consequences.

CHAPTER 4 BIOMETRICS AND NATIONAL SECURITY

The decisions on the making of National Security Determinations broadly continue to be properly made and the new Counter-Terrorism and Border Security Act is an opportunity to tighten up some of the areas where problems have been identified in the past.

I continue to be very concerned about the searching by the Ministry of Defence into the police national fingerprint database without an agreed, clearly defined lawful basis. I hope that the National Police Chief's Council will resolve this issue in the near future and I shall report the outcome. It should be noted that this relates to my point above that inter-government searching of databases should be properly regulated.

CHAPTER 5 BIOMETRIC RETENTION AND USE

The police retention and use of biometrics is gradually coming under the more uniform governance of the Forensic Information National Databases Strategy Board (FIND-SB) and this is welcome. However, the statistical information available about the retention and use of fingerprints continues to be poor, not fit for purpose and not a basis for reliable transparency.

CHAPTER 6 DELETION OF BIOMETRIC RECORDS

Compliance with the PoFA requirements on the deletion of biometric records by the police is generally good except for the continuing dispute about the basis upon which DNA samples should be kept under the CPIA exception. I still regard some forces as keeping far too many DNA samples under this exception although overall there has been an improvement.

CHAPTER 7 INTERNATIONAL EXCHANGES OF BIOMETRIC MATERIAL

The last year has been dominated by concern about the possible effects of Brexit on European exchanges and cooperation. If, in the event, the UK is excluded from the main exchange mechanisms that would have a serious effect on the police ability to deal with inter-country and international criminality. The police have been working on mitigation planning but this will not remove the risks involved.

CHAPTER 8 APPLICATIONS TO THE COMMISSIONER TO RETAIN BIOMETRICS

The number of applications by the police to retain biometrics under s63 PACE has declined this year as resource constraints have affected either the desire or ability to make applications. We continue to evaluate the outcome of these applications and a detailed report produced by ACRO is in an attached appendix.

1. INTRODUCTION

WHAT DOES THE BIOMETRICS COMMISSIONER DO?

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

2. This is the fifth Annual Report of the Biometrics Commissioner.

3. The Protection of Freedoms Act 2012 (PoFA) is the legislation which currently governs the police use of biometrics and was passed in response to a court judgment which held that previous legislation was not proportionate in the way in which it balanced the public interest in the police use of biometrics and the individual's right to privacy.[2] The new proportionality put in place by PoFA is, like all legislation, itself open to further challenge in the courts. At present we are awaiting a judgment of the European Court of Human Rights (ECtHR) on a case involving the indefinite retention by the police of DNA profiles, fingerprints and custody images from convicted persons[3]. There have also been two applications for judicial review in the domestic courts, challenging the police use of live facial image matching in public places.[4] Any of these judgments could, potentially, lead to a re-think of present legislation.

4. PoFA governs the police use of fingerprints and DNA but since PoFA was passed there has been a very rapid growth in the availability and utility of other biometric technologies. Digital facial images are now routinely collected and stored by the police and they are experimenting with live facial image matching in public places. Other technologies, such as voice recognition and gait analysis, are also being trialled by the police and a wider set of biometrics are being deployed by the private sector and to a limited extent elsewhere in government. None of these second-generation biometrics are covered by PoFA and their deployment has run ahead of governance arrangements and specific legislation. This issue is discussed further in Chapter 2 of this Report.

5. The Biometrics Commissioner is required to provide an annual report to the Home Secretary. The Home Secretary may, after consultation with the Commissioner, exclude from publication any part that he considers would be contrary to the public interest or prejudicial to national security.[5] No such exclusions have been made to this report or any previous report.

---

1 See further Chapter 4 of this Report.

2 2008 the Grand Chamber of the European Court of Human Rights (ECtHR) in *S and Marper v United Kingdom* 2008 48 EHRR 1169. For a more detailed discussion of the process that led to the passing of PoFA see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016*, Section 1.2.

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

4 Liberty are bringing a case against South Wales Police (with the Home Office as an interested party) based on alleged breach of data protection law and Article 8 of the European Convention of Human Rights. This case is now proceeding. Big Brother Watch's case against the Metropolitan Police Service (MPS) and the Home Office has, at the time of writing, been stayed pending the outcome of an evaluation of the live facial recognition trials conducted by the MPS.

5 PoFA section 21(5)

USE OF BIOMETRICS BY THE POLICE

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

7. Facial image matching by the police may involve the use of public-facing CCTV systems. The use of such systems is subject to the Surveillance Camera Code of Practice drawn up by the Surveillance Camera Commissioner, Tony Porter, a role that was created by PoFA.[7]

POFA REGULATION OF FINGERPRINTS AND DNA

8. What Parliament decided when it introduced the PoFA regime was:

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

9. 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.

10. 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. Footwear impressions are not a biometric but nevertheless they are also included in PoFA and overseen by the Biometrics Commissioner[8].

RETENTION RULES

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

- that any DNA sample taken in connection with the investigation of an offence must be destroyed as soon as a DNA profile has been derived from it and in any event within six months of the date it was taken;[9]
- that if an individual is convicted of a recordable offence their biometrics (DNA profile and/or fingerprints) may be kept 'indefinitely';

6 See http://www.gov.uk/government/organisations/forensic-science-regulator
7 See https://www.gov.uk/government/organisations/surveillance-camera-commissioner
8 Section 15 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.*
9 That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.

- that if an individual is charged but not convicted for certain more serious offences (called 'qualifying offences'[10]) then their biometrics (DNA profile and/or fingerprints) may be retained for three years; and
- that if an individual is arrested for but not charged with a qualifying offence an application may be made to the Biometrics Commissioner for consent to retain the DNA profile and/or fingerprints for a period of three years from the date that person was arrested.

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

TABLE 1: 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

Non convictions

Alleged offence	Police action	Time period
All Offences	Retention allowed until the conclusion of the relevant investigation[11] 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)[12]

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

11 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.

12 Following an initial retention period allowed for by terrorism legislation – see Appendix C. This period will shortly be extended to 5 years, once the relevant parts of the new Counter-Terrorism and Border Security Act 2019 comes into force – see Chapter 4.

PROVIDING ASSURANCE ON POFA COMPLIANCE

13. The oversight of the retention and use of biometrics in matters of national security is exercised through reviewing all National Security Determinations (NSDs) made by the police and data collection from the counter-terrorism databases. I and my Office also have regular involvement with the Counter-Terrorism Command of the Metropolitan Police Service, have visited the Police Service of Northern Ireland (PSNI) and attend various police oversight boards relating to biometrics and national security[13].

14. For other criminal matters, assurance around compliance given in previous Annual Reports was based on a number of inspection visits, some limited data collection and experience of the case working functions of the Commissioner. As a result of the Office of the Biometrics Commissioner being almost fully staffed for the first time in my tenure, this year we have visited over half (24) of the police forces in England and Wales. On visiting these forces, we have identified a range of compliance issues. The fact of our visit certainly had the immediate effect of focusing forces on whether their procedures in relation to PoFA were adequate and compliant. In some cases, our visit resulted in recommendations as to changes that would improve compliance and future visits will check how far these recommendations have been implemented. What I do not have is the power to go beyond advice and issue guidance to police forces to assist with compliance. Getting such guidance issued has been a problem (see Chapter 3).

13 See further Chapter 4 of this Report.

2. THE CHALLENGES OF NEW BIOMETRICS

15. I have previously drawn attention to the fact that the police are exploring the use of new biometric based identification capabilities. This interest has grown in the last few years as the matching ability of some new biometric systems has improved. The pace of these improvements has accelerated at an unprecedented rate[14] and the police are now experimenting with using and, in some cases, deploying these new biometric capabilities. However, legal regulation that explicitly covers the use of biometrics by the police only relates specifically to fingerprints and DNA, even though the implementation of the most recent legislation, the Protection of Freedoms Act (PoFA), is only just over five years old. This means that there is no specific statutory framework, other than data protection legislation, to provide governance for the police use of new biometrics. There are, however, police guidelines for the use of information[15] which the police have produced and can modify, to provide self-generated governance for these new biometric developments.

16. This situation has arisen because legislation that governs the use of biometrics (by the police and others) has not kept pace with the speed of technical development in biometric capabilities. Legislation failing to keep up with the pace of technical change in data use does not just apply to biometric data. Legislators around the world have spent the last year playing catch-up with the implications of global tech companies collecting huge person-centred databases and developing the analytic tools to exploit the data. This issue particularly caught the attention of legislators because the alleged use of some of these databases to influence or change voting behaviour has now developed into a wider concern about the business model underlying the collection of such large data sets.[16] Recently, the Culture, Media and Sport Select Committee published a critical report on the use of data by global tech companies.[17]

17. The concerns about the huge databases held by global tech companies and the uses made of them have fuelled a wider concern about the implications of new data processing technology. When it is being proposed that such new data analytics be used for policing then such concerns can become dystopian.[18] However, some uses of new biometrics and data analysis by the police are very likely to bring public benefits. We all have a collective interest in living in a legally ordered society and being protected from those who might seek to harm us. The police are right to want to explore new technologies that they believe can deliver such public benefits. If they do not conduct experimental trials of these technologies, then neither they nor we will have the knowledge to judge whether the claim to a possible public benefit can be demonstrated. As for the evaluation of any new technology, it is important such trials are conducted to a scientific standard that will provide a knowledge base on which informed decisions can be made and public trust on any deployment of new technology can be based. The proper evaluation of trials may be the basis upon which to evidence a case that the police use of a new biometric technology is in the public interest. Such evaluation also aids

14 As measured by the NIST vendor testing programme. See https://www.nist.gov/programs-projects/biometrics and https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

15 The principles of management of police information (MoPI) https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

16 The most extensive discussion of this can be found in Shoshana Zuboff: *The Age of Surveillance Capitalism,* London: Profile Books, 2019.

17 Digital, Culture, Media and Sports Committee: *Disinformation and 'fake news': Final Report*, Eighth Report of Session 2017-19, House of Commons HC1791

18 Films such as *Minority Report* or media reporting of what some countries are trying to do with the new technologies feed such concerns but also serve to highlight the public policy issues.

understanding of how that benefit can best be achieved. However, police use of any biometric identification system involves significant intrusion into an individual's privacy, which raises the question of how the public benefit is to be balanced against this loss of privacy.

18. The key question is who should decide that balance or what lawyers refer to as 'proportionality'? For police use of longstanding biometric capabilities (i.e. DNA and fingerprints) proportionality was decided by Parliament[19], most recently in PoFA. Without a stated Ministerial intention to propose further legislation to govern the new biometrics, one can hardly blame some police leaders for wanting to proceed under the auspices of police guidance, although not all appear to agree.[20] Certainly National Police Chief's Council (NPCC) guidance would be better than the present somewhat chaotic situation. However, the more strategic question is whether the public will retain their confidence in the police use of biometrics if the important issue of proportionality has not been decided independently, by our elected representatives, rather than the police themselves. As discussed below the police experiments with facial matching, which involve public surveillance[21], are highlighting this issue. Outside of the police, would any other body be appropriate to decide proportionality? The courts, of course, can comment on the legality of the police use of biometrics retrospectively where a challenge has been brought and their judgments in the past have led to further legislative change. Beyond that it is difficult to see anybody other than Parliament being the appropriate arbitrator of proportionality in respect of how the loss of privacy by citizens should be balanced against the exercise of a policing power.

HOME OFFICE BIOMETRICS STRATEGY

19. For a number of years the Home Office has been promising to publish a biometrics strategy and has been regularly chided for the delay in doing so by the House of Commons Science and Technology Committee. In June 2018 the Home Office published its *Biometrics Strategy: Better Public Services: Maintaining Public Trust.22* After such a wait the *Strategy* is a rather strange document. It lists a range of policy, governance and legal issues that will need to be addressed. It states that balancing the public benefits against the intrusions into privacy and personal freedoms will be central to a successful strategy by maintaining public trust. Up to this point the groundwork for a strategy has been laid. It is ambitious and contains a number of inter-locking elements. However, from this point on the document becomes a descriptive list of some (but by no means all) of the work already under way that could be part of the strategy.

20. If by a 'strategy' is meant a vision of a future beneficial state of affairs and the steps needed to achieve that vision, the issues that will have to be resolved and, how and by whom and by when that will be delivered then, after a promising start, the *Biometrics Strategy* leaves the rest of the work to the future. For example, it proposes that over the following 12 months a review of the governance and oversight of biometrics will be undertaken. By doing so there is a risk that the technical developments will continue apace and deliver the technical aspects of the *Strategy*. The success of the *Strategy* as a whole, however, is correctly identified as

19 The police have broad common law powers to prevent and detect crime. Additionally, data protection legislation and human rights jurisprudence can be applied. Nevertheless, Parliament decided that in the case of the biometrics used by the police at the time (i.e. DNA and fingerprints) that specific legislation was required to govern their retention and use, with oversight provided by an independent Biometrics Commissioner.

20 The Commissioner of the MPS Cressida Dick stated during her Vincent Briscoe Security Lecture in late 2018 "*I believe so strongly that the balance between security and privacy is incredibly important, and never for the police to decide where the slider should sit.*"

21 This may be surveillance of people attending a particular event or of all the people who pass through a particular public area where cameras are sited.

22 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

depending on a political project to gain public trust and, unlike technical delivery, that needs ongoing political leadership. Instead the *Strategy* proposes to set up a committee of officials, police representatives and those like myself with an oversight interest. I am happy to try and be helpful[23] but a committee cannot provide political leadership or political decision making.

NEW BIOMETRIC DEVELOPMENT

21. At the time of the parliamentary debates on PoFA it was known that scientific and technical development was underway on a new (second) generation of biometric capabilities both as a means of authenticating a person's identity but also potentially for forensic purposes. Indeed, the (later abandoned) development of a national identity system under the Labour administration had planned to use automated facial matching and iris matching which was, at the time, being developed for use in border control. However, there were scientific doubts that the new biometric technologies were reliable or accurate enough to meet the standards required in criminal investigations or trials. There was little appreciation at that time about how rapidly these technologies were to develop. Two factors have enabled this rapid development. The first was the growing utility and reliability of large databases pushed by global tech companies and the needs of counter-terrorism and military use. The second was the use of machine learning (or as it is often called 'artificial intelligence' or 'AI') to develop pattern-matching software. The latter depended on the former since machine learning benefits from having access to large databases to maximise its learning abilities.

22. Machine learning has only comparatively recently been used in biometric matching, but it has dramatically increased technical matching capability. This is not to say that machine learning applied for criminal justice purposes is without problems. I discussed last year[24] the problems that had emerged with biases in facial matching that were reported for some algorithms.[25] There is an ongoing scientific debate as to the cause of these biases and software developers are trying to correct them in their systems. Such further work may correct the biases but for the moment, at least, they are a problem for possible criminal justice deployment. I also discussed last year the 'black box' problem with machine learning[26]; as systems develop their pattern-matching autonomously, it is no longer clear on what basis matching is being claimed and therefore difficult for courts to judge the veracity of evidential claims. Courts may accept matching claims if supported by expert endorsement or may require that it is verified by human judgement on the claimed matching. It is also possible that further technical development will allow machine learning systems to 'explain' how they have reached their judgements. More generally, there is a difference between the technical matching capabilities achievable in laboratory tests and the results likely to be achieved in real life deployment where a large number of other variables are involved and where an element of human decision making is needed.

23 The Law Enforcement Facial Images and New Biometric Modalities Oversight and Advisory Board has now met on four occasions and has been attended on each occasion by myself or my Head of Office. https://www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board#minutes

24 See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2017*, paragraph 318.

25 https://www.nist.gov/sites/default/files/documents/2017/11/20/grother_11_02_bias.pdf

26 See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2017*, paragraphs 316-317.

POLICE USE OF NEW BIOMETRICS – FACIAL IMAGES

23. Of the new biometric technologies being developed the earliest to be used by the police was facial matching. Ever since the development of photography the police have used facial photographs ('mug shots') of arrestees for subsequent identity checking, investigation and for tracking down alleged offenders. The more recent development of digital photography meant that facial images could be stored on a searchable 'national' database[27] and the development of facial matching algorithms opened up the possibility of automating the searching capability.

24. Following the Bichard Inquiry Report[28] into the Soham murders, the Home Office created a new database – the Police National Database (PND) – so that in future the police would be able to share intelligence and other information about offenders nationally, since the lack of such a capability was identified by Bichard. Under the leadership of the Chief Constable of Durham Police, PND has subsequently been used to store digital custody facial images of arrestees and has also had facial matching software added. This national facial image database and image matching is available to police officers across the UK, but is still developing, since not all police forces are currently uploading their custody images to PND due to local technical difficulties that are being worked on. Further, not all of the images that are uploaded are of sufficient quality to be used by facial recognition software. Presently PND contains approximately 23 million images[29] of which around 10 million are technically suitable facial images of sufficient quality to be searchable.[30] The police use facial images as a biometric identifier under general policing powers. However, the legality of the *retention* of custody images was challenged and in a 2012 judgment the High Court held that the continued retention of images from unconvicted individuals under the Metropolitan Police Service's policy for the retention of custody images, which followed the Code of Practice on the Management of Police Information and accompanying guidance ('MoPI'), was unlawful without case by case consideration.[31]

25. The Home Office eventually responded to this judgment by publishing, in 2017, a Review of the Use and Retention of Custody Images.[32] At the time this seemed a rather limited response in that it did not suggest a set of new, automatic rules for the retention and use of custody images by the police either locally or on PND. Rather than introducing automatic weeding of images to match the proportionality required by the judgment, the Review essentially reiterated that the time periods for review of information about an arrestee as set out in MoPI, depending on the offence, should be applied specifically to custody images. Additionally, the Review introduced a right for an arrestee to make a request to a Chief Officer for their facial image to be deleted, with a presumption of deletion in certain, limited circumstances. Essentially, the current position for a person arrested for but never convicted of an offence is that the retention of their image should be reviewed after six years, unless they make a specific request for it to be reviewed sooner. Last year I questioned whether the Review's proposals would withstand further court challenge. It later transpired that one of the reasons why the Home Office had

27 The Police National Database (PND) contains a 'national' database of custody photograph images. However, a significant number of police forces do not currently upload their images to this database, so it cannot be said to be a truly national database at present. See also paragraph 26 below.

28 Dera.ioe.ac.uk/6394/1/report.pdf

29 This includes images of marks, scars, tattoos and some low-quality images that cannot be searched, bringing the actual number of custody images down to around 15 million.

30 Around 15 million of the images are technically searchable but only around 10 million can actually be searched and give a useable result. Figures provided by Home Office Digital, Data and Technology.

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

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

not proposed automatic weeding of custody images, particularly those on PND, was that they claimed it was not technically possible to implement such an automated process. This was confirmed by the Minister in a hearing before the Science and Technology Select Committee.[33]

26. Whilst the police have developed this capability to nationally store and digitally search and match facial images, the system has a number of limitations. The utility of a national database of facial images depends on having images of sufficient quality to maximise matching ability. At present not all police forces are capturing images of sufficient quality to be included on PND and not all police forces are capturing images of a uniform standard. A national facial images database would be expected to contain images from all forces but, as explained above, at present it does not. The facial image database also needs to be able to interact with police data on offending and conviction history if rules on retention and deletion, based on police investigation and prosecution outcomes, are to be implemented and automated, but this is currently not the case. These technical problems will remain until the new Home Office replacements for both PND and PNC become operational[34] and all forces are persuaded to capture facial images of sufficient quality and upload these to the national database.

27. In the meantime, the processes proposed by the Home Office Review of the Use and Retention of Custody Images were handed to the College of Policing to implement. The College's recommended process for responding to requests to Chief Officers for the deletion of facial images can be found on their website.[35] The recommendations implement the guidance given in the Review but are quite restrictive and depend largely on the discretion of the Chief Officer. This year we have visited over half of the police forces in England and Wales and we have found very little awareness of the deletion process, very few applications requesting deletion and therefore few deletions. We also found little awareness of the periodic reviews of facial image holdings recommended in the Review and implemented by the College of Policing in their current APP on the Management of Police Information (MoPI). Further, as far as we can ascertain from speaking to police forces, few such reviews are being carried out. Not only, therefore, was the Review rather limited in its response to the RMC judgment but even the limited proposals made in that Review have not been fully adopted by the police.

POLICE TRIALS AND EXPERIMENTS

A number of policing bodies have approached my office seeking guidance because they are in the process of starting early trials of new biometric technologies and they want to know what rules or governance framework they should be applying. Their queries are a commendable desire to ensure that their developments are lawful but also a pragmatic understanding that bolting on governance rules after technical development is much costlier than developing technical solutions within known rules. The problem is that there is no legislation specifically covering the retention and use of the new biometrics in which they are interested. Strictly, my own oversight is limited to specific biometrics (i.e. DNA and fingerprints) and all I have been able to suggest is that in addition to police guidance, some general principles on the police use of biometrics can be derived from the PoFA rules on the retention and use of DNA and

33 Baroness Williams of Trafford, the Minister of State for Countering Extremism, gave evidence to the House of Commons Science and Technology Select Committee on 6 February 2018, followed up by a letter dated 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

34 The Home Office's National Law Enforcement Data Programme (NLEDP) is responsible for developing and delivering the much-needed replacement for PNC and PND. I understand that there have been significant problems with the programme and that delivery is still some years away.

35 https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#group-1-certain-public-protection-matters

fingerprints by the police. For example, one might extrapolate from PoFA that police retention of biometric data should be proportionate to the outcome of any previous contact with the criminal justice system. In addition, of course, I have pointed them to the requirements of data protection legislation.

EXPERIMENTAL FACIAL MATCHING IN PUBLIC PLACES

28. The police trials of new biometric technologies that have particularly drawn attention from both the news media and civil liberties groups are those trialling the use of live time facial matching by public surveillance[36]. These trials have been carried out in a Home Office-funded trial by South Wales Police and by the Metropolitan Police.[37] The capability being trialled is broadly the same in both cases. A relatively small local 'watch list' is constructed from custody images either of those wanted on a court warrant or as part of a serious crime investigation or those deemed to be a threat at a particular event, such as a sporting event or other public gathering. Cameras are then set up either in a local area with significant pedestrian traffic or on the approach to the event being used in the trial. Usually a pedestrian 'pinch point' is chosen so that the cameras can scan the crowd whilst facial matching algorithms search for matches to the watch list being used. If a possible match is found this is relayed to police officers who make both a human visual check against the custody image and a check against other police databases. If the possible match is confirmed this is relayed to officers downstream of the cameras to stop the individual and carry out further checks. In addition, some police staff may be added to the watch list and then walk through the scanned area, in order to establish how far a known match is actually found by the systems, what is often referred to as establishing a 'ground truth' measure of matching success.[38]

29. These trials are clearly limited in what they can establish but they will show whether such a public use is technically possible. An initial evaluation of the South Wales trial has been published[39] and an evaluation of the Metropolitan Police trial is awaited.

30. However, the main concern that these trials have generated has not been about their scientific quality but about the legality of the police use of cameras to scan the general public against a police facial image database[40]. Two civil liberty groups, *Liberty* and *Big Brother Watch*, have sought judicial review against South Wales Police, the Metropolitan Police and Home Office, challenging the legality of the police action. Their concern is that the mass scanning and processing of the images of people in this way in public places is not proportionate as it constitutes a significant interference with the Article 8 rights of those affected and that such interference is "not necessary in a democratic society" or "in accordance with the law" under the European Convention on Human Rights (ECHR)[41]. We shall have to await the court judgments, but these cases are probably only the first challenges to the police use of new biometric technologies in trials. Actual deployment of new biometric technologies may lead to more legal challenges unless Parliament provides a clear, specific legal framework for the police use of new biometrics as they did in the case of DNA and fingerprints.

36 This may be surveillance of people attending a particular event or of all the people who pass through a particular public area where cameras are sited.
37 Some other forces have also experimented with working with private organisations, such as shopping malls.
38 I am grateful to Commander Ivan Balhatchet of the MPS for allowing me to observe one of these trials.
39 https://crimeandsecurity.org/feed/afr
40 There are various legal frameworks within which the police can claim be able to operate such systems, including common law powers, data protection legislation and relevant human rights jurisprudence. The use of public facing camera systems is further subject to the Surveillance Camera Code of Practice, overseen by the Surveillance Camera Commissioner.
41 In addition, it is argued that the use of AFR also breaches articles 10 and 11of the ECHR and is unlawful under section 6 of the Human Rights Act 1998.

31. What is not yet clear is how the police might want to eventually use such public surveillance following on from the trials. The trials have been matching against small watch lists. Matching against entire police national databases or national watch lists would be more challenging but in future may be technically feasible. It could be argued by the police that searching for those wanted on a court order or as part of a serious crime investigation using a nationally generated watch list has public benefit by making justice more certain, but whether that justifies such extensive surveillance is open to question. Further, the police could claim that checking identity via a facial image in situations where the police have reasonable grounds to stop a person for such a check is simply an alternative to the current police use of mobile fingerprint scanners for this purpose[42]. In a similar way it may be held that the use of surveillance against local watch lists is in principle little different than the long established practice of posting wanted notices or briefing patrolling officers to look out for wanted persons. Widespread surveillance on the other hand, even against a local watch list, is a significant intrusion into the privacy of all those scanned with a very small probability that they will be matched to the watch list. In addition to possible uses of public facial scanning there are questions about what is done with the images scanned and templated for matching and particularly the matched images. My understanding in the trials is that the images only of those who generate a claimed match against the watch list are retained but the retention policy needs to be clear before any operational use, just as it needs to be clear whether the police intend to capture new facial images during surveillance and on what legal basis they would do so.

32. The police use in public places of this first of the new biometric technologies (i.e. the matching of facial images in real time) has already created controversy. At its extreme it is raising the spectre of using facial scanning for mass police surveillance. That may be unlikely but one that some countries are reported as developing.[43] The sober point is that unless there are clear and publicly accepted rules governing the police use of new biometrics then damage could be done to public trust in policing and at a time when regard for some other public institutions is declining.[44]

PRESENT GOVERNANCE OF NEW BIOMETRIC USE BY THE POLICE

33. Outside of specific legislation on the police retention and use of biometric data (fingerprints and DNA under PoFA) there is other governance that applies.

34. The first of these is the new Data Protection Act 2018 which broadly requires any organisation using data to abide by the 'data protection principles'[45]. The Information Commissioner can investigate if she believes that these principles are not being properly followed and she also possesses enforcement powers. The Data Protection Act 2018 provides some limited exemptions from these requirements for some government (and particularly law enforcement) activity but nevertheless the police use of biometric data is generally subject to the same overriding principles of lawfulness, fairness, legitimacy, accuracy, security, timeliness and relevance[46]. Data protection legislation does recognise biometric data as particularly sensitive as regards its intrusion into individual privacy. It should be noted, in particular, that it defines

42 This can be done under PACE powers where the police doubt the identity of an individual.
43 According to press reports China has claimed such surveillance.
44 Trust in many public bodies has been declining in many countries and reviews of new technologies by the Government Office for Science has often pointed to the importance of trust in and public acceptance of technical innovation.
45 https://www.gov.uk/data-protection
46 See also Appendix D

'biometric data' as including not just biologically derived data but also behavioural data.[47] In other words, 'biometric data' is extended beyond the police use of biologically-based systems to their use of person-centred behavioural data which may include the police's current development of data analytics – the Home Office funded National Data Analytics Solutions (NDAS) programme.[48]

35. All police forces have needed to review their use and retention of data in order to comply with the new data protection legislation. For example, forces must respond to requests by individuals to be informed if any data about them is being held by the police and its purpose. Concern about the police developments in facial matching has resulted in the Information Commissioner's Office (ICO) currently examining the police use of such data and they will in due course publish a report of their findings.[49] The ICO can issue guidance which, if they do so, will be influential in the governance rules put in place by the police.

36. In addition to data protection legislation, the police follow the governance laid out in the Management of Police Information (MoPI), which was originally drawn up by the Association of Chief Police Officers (ACPO) but with the demise of that body it is now drawn up by the College of Policing.[50] MoPI guidance must be compliant with legislation[51] and seeks to balance necessity and proportionality. In other words, the police are deciding the balance of necessity and proportionality where specific rules regarding a particular biometric or use of that biometric have not been laid down in statute. Absent that balance being provided in statute in relation to the retention or use by the police of biometric data (i.e. any biometric other than DNA or fingerprints) then it is not unreasonable for the police to make that judgement, but it leads to two questions. First, should the police be making these decisions as the body which also want to gain the benefit of using the new biometric? Secondly, will the public accept that this should be entirely a police matter, or will that undermine the public's trust in the police use of biometrics? Initially that is a strategic matter for police leaders.

37. One might expect police generated guidance to follow, in principle, the approach laid down in PoFA. In the case of the retention and use of custody images there is some dispute as to whether following the rules already established in PoFA ought to be the way forward. Some police leaders have argued that the retention and use of facial images should not be governed by the same rules used in PoFA for fingerprints and DNA. They argue that custody images are used for different purposes than DNA or fingerprints, namely to inform officers about the risks presented by some individuals and that the retention of a person's facial image – even, where that person has never been convicted of a criminal offence – is necessary for risk-management by the police to protect themselves and others or prevent and/or detect future offending. The argument therefore is that PoFA rules, which generally allow retention of biometrics based on the outcome of the legal process, are therefore not appropriate and instead retention decisions for custody images should be based on police intelligence and what is known about the previous behaviour of the individual and the risks they are believed to present. In other words, this should be a police intelligence-based process rather a criminal justice-based policy. Given these differences then the proponents conclude that governance

47 Biometric data '*means personal data resulting from specific technical processing relating to the physical, physiological or* ***behavioural characteristics*** *of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;'* GDPR, Chapter I, Article 4, paragraph 14

48 See paragraphs 47-48 below.

49 See the Information Commissioner's letter to the Science and Technology Committee: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.html

50 See https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

51 Such as PoFA and data protection legislation and the ECHR, although it is yet to be updated in the light of the Data Protection Act 2018.

should come from a police-led process such as those currently provided by MoPI[52] rather than a legislative framework with a concrete set of rules based on the outcome of the legal process (for example whether the individual is charged or convicted of an offence). Governance based on the outcome of a legal process is easily turned into rules that are objective, publicly visible and subject to oversight. Governance in relation to police risk judgements is less amenable to producing objective rules which are publicly visible and subject to oversight.

38. At heart, the question both in relation to this specific case and more generally is whether the public interest case for retaining and governing the police use of facial images put forward by the police is acceptable when set against the intrusion into privacy. We all have an interest in the answer to that question and for that reason it is debatable whether the answer can be left to the police themselves. This is not to impugn the integrity of the constabulary but simply that a public interest case requires a public answer. Even if the police's public interest case is accepted it does not follow that the police should decide the governance process. Of course, the police can rightly point out that whatever process they design will be subject to the general rule of law (and indeed specific statutes such as data protection legislation)[53] and can be legally challenged so their freedom in this matter is not absolute. Moreover, the police might reasonably conclude that if their use of biometrics was a sufficiently important public issue then government would act to decide the governance framework. In the past the use of biometrics in the criminal justice process has been judged as sufficiently intrusive of individual freedom and privacy and that Parliament ought to decide how the public interest in a biometric use by the police should be balanced against the intrusion in an individual's life.

39. There are a number of different operational uses to which the police might apply a new biometric and the public interest justification may vary from case to case, and in turn lead to different proposals as to governance. However, if that in turn leads to a plethora of rules to reflect these differences then legislation will simply not keep up and will result in such legislative complexity as to make compliance difficult by overburdening front-line officers with rule complexity. The same difficulties would arise if governance is provided by a plethora of police codes. On the other hand, if some general principles for the police use of biometrics can be agreed then any necessary variation in rules needed to cover a particular biometric use can be derived from those principles. If this can be done, then legislative control of the process of technical innovation can achieved. Furthermore, it will provide for ease of application of the rules by the police and therefore compliance to a publicly understandable legal framework. On such a framework public trust in the police use of biometrics can be built.

NEW LEGISLATION?

40. This situation has arisen because legislation that governs the use of biometrics (by the police and others) has not kept pace with the speed of technical development in biometric capabilities. Legislation failing to keep up with the pace of technical change does not only apply to the police use of biometrics but more generally there is growing concern about the uses to which personal data is being put and whether it serves the public interest or a sectional interest. We have entered a world of powerful data analytics at a speed that has not allowed for a public debate as to how this new capability can add to human social flourishing. Indeed, we are just coming out of a period of public policy ignorance as to how intrusive and pervasive the new

52 https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#group-1-certain-public-protection-matters

53 The principles of the ECHR must also be applied. Additionally, the case of live time facial matching for example is subject to the Surveillance Camera Code of Practice, overseen by the Surveillance Camera Commissioner.

data analytics are and whether such powerful, global and fast-moving technology can be controlled by nation states through legislation. As is often the case with rapid and disruptive new technology, legislators first need to escape from technological determinism before they can decide how to act.

41. It would be difficult for legislators to continually pass laws in order to keep up with the speed of technical changes, for example to ensure that each new biometric capability is subject to appropriate governance and oversight. If they were to try they would inevitably fall behind. One answer is to try and develop legislation that is flexible enough to cope with changing technical capabilities. In the last year there have been two attempts to provide this kind of legislative framework. They are the Data Protection Act 2018, and the Scottish proposal for new legislation to regulate the police use of biometrics which is to go before the Scottish Parliament later this year[54]. Both use similar legal architecture: they set out general principles for the use of data or biometrics and create a body whose function is to ensure compliance and interpret the application of the principles, including in response to technical change. In the case of data protection legislation, the principles are provided by the European Union's General Data Protection Regulation (GDPR) together with the Law Enforcement Directive which was then given domestic legal expression in the Data Protection Act 2018 with compliance and interpretation provided by the UK Information Commissioner. In the Scottish proposals, it is suggested that legislation will lay down principles with interpretation and compliance guided by a code of practice drawn up by a Scottish Biometrics Commissioner, answerable to the Scottish Parliament. These approaches attempt to provide for flexibility in the governance of new data/biometrics or new uses of data/biometrics, encompassed within the principles set down in the primary legislation.[55]

42. Home Office Ministers currently show no sign of proposing a new legislative framework with specific rules to govern the police use of new biometrics in England and Wales. I do not know whether this is because they disagree with the need for such legislation or whether this is just another casualty of the need to focus on Brexit matters.

43. In addition to whether there should be legislation to govern the police use of new biometrics there are also questions about the governance of the Home Office's new data platforms and the police development of new data analytics.

THE NEW HOME OFFICE DATABASES

44. There is currently a need for both clarity and governance of the developing Home Office Biometric (HOB) programmes and the searching into police databases by other public bodies. The Home Office are in the process of replacing their elderly databases. This is being done by the Home Office Biometrics Programme (HOB) to replace existing Home Office biometric databases such as the national fingerprint database, IDENT1 and its sister programme, the National Law Enforcement Data Programme (NLEDP) to replace the Police National Computer (PNC) and the Police National Database (PND).

45. In the first instance the work being done by HOB will involve providing direct replacements for existing Home Office databases but these will be hosted on new generic biometric data platforms. For example, the police fingerprint databases and the immigration fingerprint

54 https://www2.gov.scot/About/Review/biometric-data

55 Some commentators have pointed out that this approach may come more naturally to Roman-based lawyers rather than English common lawyers – a point made by Her Majesty's Inspector of Constabulary, himself a trained Scottish lawyer.

database will both be hosted on a new fingerprint data platform. In future these new data platforms could also host other government databases. The individual collections on each data platform will be logically separated in the data architecture so different governance rules can be applied for the use of and access to each collection. These logical separations will in the first instance reflect the existing practice for each database. However, these practices vary as to whether their basis is found in legislation or not and how access for third parties can be agreed. Before these data platforms are made available to others there need to be clear rules to regulate future inter-governmental access to databases. It seems to me imperative that this be resolved before such multi-user data platforms are completed and brought into use. The recent Home Office Biometrics Strategy[56] discussed some of this but did not make clear the extent of the ambition behind the HOB programme or how governance arrangements would apply, nor whether these would need legislation.

46. There is nothing inherently wrong with hosting a number of databases on a common data platform with logical separation to control and audit access but unless the governance rules underlying these separations are developed soon then there are clear risks of abuse. This risk has already crystallised. IDENT1 was originally developed purely to hold the police national fingerprint databases but subsequently the Ministry of Defence were allowed to add their fingerprint database to IDENT1, albeit in a separate 'cache'. What does not seem to have happened when this was agreed was to establish clear access rules to the different databases held on what was now a multi-user data platform. Three years ago the Chair of FIND-SB discovered that the MoD was searching into the police national fingerprint databases without a clearly evidenced lawful basis for doing so. This is discussed in detail in Chapter 4 of this report and it illustrates why I regard it as urgent that access rules and appropriate governance arrangements are decided upon and implemented before the new HOB data platforms come into use.

THE POLICE NEW DATA ANALYTICS PROJECT

47. The Home Office is funding a National Data Analytics Solutions (NDAS) proof of concept project. The project involves a number of police forces with the purpose of exploring how far new data analytics (and especially machine learning) can make existing police data more useful in addressing current problems, for example, to take a current issue, identifying the offender risk factors associated with violent knife attacks. At present the programme is not collecting new data, nor using data other than that already held by the police. The funding for the present work comes to an end shortly and so its future is uncertain. Exploring the utility of police held data about both victims and offenders is not new, for example mapping crime victimisation has been used to try and prevent repeat victimisation and both Probation and Youth Justice have used risk assessment tools to guide their work with convicted offenders. As with biometrics, it is the new analytic power that machine learning brings to such work that potentially will change the scope of such work by the police.

48. I have been impressed with how carefully the present NDAS programme has thought through how such analytics should be used, especially the danger of bias and what limitations there should be on the use of any predictions which relate to the risk presented by an individual. However, separately to the NDAS programme, a number of vendors are offering predictive algorithms which they claim can make these type of predictions and *Liberty* has raised concerns about the use of such predictive software and the danger of it re-enforcing existing

56 https://www.gov.uk/government/publications/home-office-biometrics-strategy

biases in policing[57]. Essentially, the use of such new analytics will raise many of the same issues as have been discussed above in relation to facial image matching, as will the use of any other new biometric technology. Indeed, insofar as these new analytics use personal behavioural data, they will fall within the data protection legislation definition of 'biometrics'. The use of machine learning (or artificial intelligence) to drive such analytic work is a common thread that links new biometrics and the much broader problem of the uses that can be made of very large databases now being held by both governments and private companies. There are some problems specific to this new technology, such as possible biases and the 'black box' problem of how the analytics are working. However, the main problem is what such analytics are being used for and whether that is in the public interest, and if not how they can be regulated or controlled. That is a common problem of both biometrics and machine learning analytics.

NEW TECHNOLOGY AND NEW POLICING CAPABILITIES

49. In summary, we are seeing the rapid exploration and deployment by the police of new biometric technologies and new data analytics. Some of these will improve the quality of policing and will do so in a way that is in the public interest. However, some *could* be used in ways that risks damaging the public interest, for example by re-enforcing biases of which reinforcement is not in the public interest. If the benefits of these new technologies are to be achieved there needs to be a process that provides assurance that the balance between benefits and risks and between benefits and loss of privacy are being properly managed. Several fragmented processes and rules for different biometrics or data analytics will, in my view, be too complex and opaque to engender such trust and purely police-determined policy decisions will always be open to the doubt of self interest. This is a major public policy issue which will influence trust in policing for some time to come and our tradition of policing has always been tied to public trust. As such the principles that guide the governance of these developments ought to be decided by Parliament and expressed in law.

57 https://www.bbc.co.uk/news/technology-47118229

3. CHANGE IN POLICING AND UNINTENDED CONSEQUENCES

50. The Protection of Freedoms Act 2012 (PoFA) was unusual in that it created the role of Commissioner for the Retention and Use of Biometrics (Biometrics Commissioner). The Commissioner has some decision-making powers in relation to applications made to him under section 63 of PACE and the awarding of National Security Determinations. In addition to these powers the Commissioner is required to report annually to the Home Secretary on the working of PoFA and that report is subsequently laid before Parliament. PoFA therefore is one of the few pieces of legislation whose workings have been monitored and reported on since its commencement, so Parliament can judge how far the legislation has achieved their purpose(s) at the point of legislating. During the time of the first Commissioner most of the issues which arose were about clarifying the meaning and application of some sections of PoFA and providing guidance or technical means to ensure compliance. Such work is probably required during the implementation of any new legislation, but this has continued under my time as Commissioner and the last significant issue of this kind was only (partially) resolved during the current reporting year[58]. In other words, it has taken 5 years to achieve broad compliance with the legislation and even now some promised guidance has still not been issued[59] despite the Minister with responsibility for biometrics repeatedly stating that guidance would in future be produced in a timely manner[60].

51. Moreover, the 2015 Annual Report observed that there were a number of serious and equivalent offences that had seemingly been omitted from the list of qualifying offences as set out in section 65A PACE.[61] Some law enforcement agencies also wanted the list to be extended, for example the National Crime Agency (NCA) wanted to see serious fraud added since they are often investigating serious international fraud and biometrics can be important in such cases. 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, but this has been repeatedly delayed and it remains unclear when this will happen, although I am advised that Parliamentary time may be available in late 2019.

52. More recently, however, a number of new issues relating to the police capture, retention and use of biometrics have arisen. Firstly, other changes in policing have had unintended consequences for the retention and use of biometrics, the most serious of which is a decline in new biometric material being added to the national databases, which may have a significant effect on their future utility. This raises the question of whether such consequences could reasonably have been foreseen. Second, new biometrics are being deployed by the police without a clear, specific governance framework or Parliamentary discussion about proportionality. Third, a new technical infrastructure for holding government national biometric databases is being created, again without clear governance rules or an overall government strategy nor a clear, specific legislative framework. Finally, the police are developing new data analytics capabilities

58 See Chapter 4, paragraphs 92-94 on s18 retention of national security biometrics.

59 No guidance has yet been issued on the meaning of 'indefinite retention', the CPIA exception, 'under investigation' markers or retaking fingerprints and DNA from an arrested person. See also *Commissioner for the Retention and Use of Biometric Material, Annual Report 2017,* at paragraphs 41-44 and 62-63. Further, the provisions of section 70 of the Crime and Policing Act 2017 were commenced on 03 April 2017 but the Home Office have not yet completed the work needed for these changes to be brought fully into effect on the PNC or issued the necessary guidance. See also Appendix A.

60 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/713593/government_response_-_annual_report_2017.pdf

61 See Commissioner for Retention and Use of Biometric Material, Annual Report 2015 at paragraphs 65-67.

which, if they use behavioural data, are within the definition of 'biometrics' used in the Data Protection Act 2018. The first of these is issues is discussed in this chapter and the others in the previous chapter.

53. Whilst PoFA provides a specific legal framework for police retention and use of biometrics (DNA and fingerprints), other changes to legislation and associated statutory codes have had unintended consequences. These unintended consequences have been highlighted in previous Annual Reports by both myself and my predecessor[62] but it is only this year that we begin to fully appreciate the impact of these on the number of fingerprints and DNA profiles being captured and added to the national databases.

54. Two changes that appear to be having a significant effect are:

1. On 12 November 2012, Code G of the Police and Criminal Evidence Act 1984 (PACE) changed for the first time since 2005, in response to a number of decisions in which the courts clarified the law on the necessity of arrest and, in some cases, found arrests to be unlawful[63]. In particular:

   (i) Where a police officer needs to interview a suspect, they must now consider whether a voluntary interview would be practicable. If it is, then arrest would not be necessary and may be unlawful; and

   (ii) The necessity criteria do not permit arrest solely to enable the routine taking, checking (speculative searching) and retention of biometrics. There must be reason for the officer to believe that taking such samples would provide evidence of the person's involvement in the offence, or help to determine their identity.

2. The Policing and Crime Act 2017 contains a provision, which came into force on 3 April 2017, that introduced an overriding presumption of release without bail unless strict necessity and proportionality criteria are met. Additionally, pre-charge bail is now limited at 28 days, with extensions available in exceptional circumstances[64].

55. The problems that the police and others have been experiencing – and that I set out below – as a result of these changes, might well have been mitigated if the Home Office had fully considered the operational consequences of the changes that were made both at the time of drafting the proposed new Code G and the Policing and Crime Act, or before they were implemented. They might, further, have been mitigated by allowing the police a transition period during which to make the necessary changes to their processes and IT systems, in order that they be able to comply with the new legal requirements. Most significantly, in my view, the police ought to have been provided with guidance as to the precise interpretation of the new Code and legislation and how, operationally, this was intended to be implemented. Instead, what we have seen is a period of confusion, inconsistency of approach nationally and a series of seemingly unintended consequences, which may well pose a serious risk to both the rights of suspects and the safety of the public.

---

62 See in particular Commissioner for the Retention and Use of Biometric Material, Annual Report 2017, at paragraphs 83-94.

63 *Richardson v The Chief Constable of West Midlands Police:* QBD 29 Mar 2011

64 There are three main applicable bail periods that the police can authorise:
1. Initial applicable bail period for 28 days authorised by an inspector.
2. An extension to the initial applicable bail period, to three calendar months from the bail start date authorised by a superintendent.
3. A further extension to the applicable bail period of three calendar months for cases designated as being exceptionally complex, authorised by an assistant chief constable or commander.

All further extensions to the applicable bail period must be authorised by a magistrates' court.

56. In relation to voluntary attendance it has taken over six years for national guidance to be issued. Part of the reason – to which I have previously drawn attention[65] – for this delay is a disagreement between the Home Office and the police as to who should produce and issue guidance as to the operational interpretation of legislation. The police take the view that the Home Office should provide guidance on legislation for which they have been responsible whilst the Home Office take the view that new legislation having been passed, it is for Chief Officers to determine how the legislation should be implemented. It is not for me to resolve this disagreement but it does mean that guidance to the police to help them resolve issues around the practical implementation of legislation, and thereby a coherent national policing approach, can be long delayed. There has, further, been a failure by the Home Office to issue guidance where it has been promised and/or a refusal by the Home Office to issue guidance where it considers something to be a police matter. On the police side the National Police Chiefs Council (NPCC) seems to lack a clear structure for the creation and endorsement of guidance. These same difficulties were identified in recent criticism by the Home Affairs Select Committee of the failure of the Home Office to set policing policy and the difficulties for the police in taking a national approach, given the fragmented system of policing; views with which the Policing Minister *'appeared to have sympathy'*.[66]

VOLUNTARY ATTENDANCE

57. Prior to the 2012 changes to Code G the majority of suspects being investigated by the police were arrested. Since the revised Code G was introduced, constraining the police in their use of arrest powers, the use of arrest has gradually declined and police forces are now routinely reporting to me that around one third of suspects who are questioned are not arrested. Suspects who are not arrested will be asked to attend voluntarily, at a specific time and place, to answer police questions and are commonly known as 'voluntary attendees' (VAs). VAs may be interviewed anywhere that has appropriate recording equipment for example at a local police station or even at their home[67]. Being dealt with via the voluntary attendance process means that the suspect will not usually enter a police custody suite, indeed it is intended that they should not do so.

58. During the visits made by my Office this year to 24 of the 43 police forces in England and Wales there have been extensive discussions about the use of voluntary attendance. Whilst forces report that their move from arrest to voluntary attendance was initially driven by the changes to Code G most also cite other reasons that are related to increasing financial pressures. Many forces, for example, are rationalising their custody estates; significantly reducing the number of custody suites in order to improve efficiency and cut costs.[68] In forces that cover a large geographical area this can mean taking a suspect a significant distance to the nearest custody suite following arrest, which is costly in terms of time and money. Interviewing that same suspect as a VA rather than an arrestee solves that problem. Furthermore, the administrative work and time spent for an officer in processing a VA who attends, with their solicitor, at a pre-

65 Commissioner for the Retention and Use of Biometric Material, Annual Report 2017, at paragraphs 88-94
66 https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51513.htm#_idTextAnchor100
67 Interviews can now be recorded on body worn video if this has been authorised by the Chief Officer in a police force. This has been the case since changes were made in May 2018 to Code E of PACE. The Code does not specifically refer to body worn video but such devices may be used if they comply with the revised operating specifications and associated manufacturers' instructions and the interview is conducted in accordance with the Code.
68 The increasing use of voluntary attendance has had the concomitant effect of reducing the flow into custody suites so reducing their economic viability.

arranged time is far less than for an arrestee being taken into and interviewed in custody. There are therefore significant cost and time savings for stretched forces and individual officers, thus a further pull factor in favour of using voluntary attendance rather than arrest.

59. Police forces have also reported to my Office that the changes to the use of pre-charge bail made by the Policing and Crime Act have contributed to the increased use of voluntary attendance. Prior to these changes one expected outcome of arrest was that the suspect, if there was not an immediate resolution to the case, would usually be released on bail. Given that this is no longer the case, a further impetus to arrest a suspect rather than deal with them as a VA has been lost.

60. In many cases the use of voluntary attendance to handle a suspect may well be the most appropriate course of action, as arrest would not be necessary or proportionate. Indeed, it may be especially desirable and beneficial where the suspect is very young, has vulnerabilities or it is their first contact with the criminal justice system. I am concerned, however, that some suspects are being dealt with as VAs when it could well be argued that it is necessary and proportionate for them to be arrested. In particular I have observed that:

    a. Many forces have no specific policy and/or guidance for officers to assist them in making a decision as to whether it is practicable for the suspect to be a VA. Even where there is guidance it seems that in many forces officers are still not well informed about the process, do not understand the guidance, are not supported to follow the guidance or do not have time to make a proper consideration.

    b. Voluntary attendance is currently being used for a wide variety of offences, including sexual offences (including rape) and violent offences, some of which may be inappropriate both in terms of failure to capture biometrics and managing the risks to the suspect, victim and wider community. I am particularly concerned that there appears to be a widespread view that suspects facing allegations of historic sexual offences should be VAs. Without using arrest a speculative search of the subject's biometrics can not be made and one route for determining if there is any possible further risk is missed. There may also be necessity in terms of safeguarding the suspect from causing harm to themselves prior to the interview.[69]

    c. In some forces the facilities for interviewing VAs may not be well equipped and have no access to services such as a custody nurse or mental health services. The risk to the suspect caused by this is not always being fully assessed and/or mitigated.

61. If a suspect is a VA then their biometrics cannot be taken at the outset as they would be when someone is arrested, since there is no legal power to do so under PACE (as amended by PoFA). There has been a degree of confusion about this for a number of years and a very inconsistent approach nationally to taking biometrics from VAs. Some forces have been taking biometrics inappropriately from VAs, for example before their interview, subsequently discovering that they are unable to load them to the national databases as there is no legal basis to load, search or retain them. A small number of forces have been reporting every VA straight after the interview, wherever they think there is the slightest possibility the case will proceed, so that they can then take the biometrics at the time of the interview. The NPCC formed a working group to consider the use of the voluntary attendance process and have recently issued some national guidance. The guidance in relation to biometrics is to the effect

69 We have had one such case reported to us.

that biometrics should be taken only if the VA is subsequently issued with a notice of intended prosecution (frequently a postal charge). Any force that took biometrics earlier in the process will now have to consider re-visiting cases in order to avoid unlawfully held biometrics leading to unlawful matches.

62. The confusion as to when biometrics can be taken from VAs has been partially cleared up – although my Office is still receiving queries from forces about interpretation of the guidance which does not bode well – but that still leaves a practical problem. If a suspect is arrested and taken to a custody suite then their biometrics are captured by trained custody staff whilst they are in custody, before they are interviewed. For VAs, however, their biometrics may not be taken when a person is initially interviewed but only later if the police decide to proceed with a prosecution. This frequently occurs long after the suspect has left the police interview.[70] Nevertheless, it appears that some police forces currently have no process for subsequently identifying suspects from whom they may lawfully obtain biometrics and many have no process in place to ensure that biometrics are captured from VAs at a later date where permitted. Sometimes this is left to individual officers, who are encouraged to follow up and take biometrics and other times there is no feedback process at all. As a result some police forces report that they are rarely capturing biometrics from any of their VAs, even where there is a lawful basis for doing so.

63. The new NPCC guidance suggests that suspects are sent a letter, together with any postal charge letter, informing them that they must report to have their biometrics taken. They should then be given seven days to do this (although there remains some uncertainty around whether the suspect may be given a specific time to attend) and if they fail to do so having been given adequate opportunity they can, if necessary, be arrested in order to obtain their biometrics. Some forces already have a process in place for writing to suspects but few have processes in place to ensure compliance. I am only aware of one police force, Greater Manchester Police, where biometric capture from VAs (where appropriate) is achieved in almost 100 per cent of cases. This has been achieved, after a great deal of thought and planning, through having a small team that is solely responsible for this process. Manchester also has the advantage of being, geographically, a relatively small area with good public transport links to its several custody suites. In a geographically large rural force, with poor transport infrastructure, ensuring this level of compliance with biometric capture would be a great deal more difficult.

64. A further difficulty arises, again exacerbated by the rationalisation of the custody estate, (particularly in geographically large rural forces) that if a suspect reports to a police station that does not have a custody suite there will be no facilities to take fingerprints using Livescan machines[71] which, when operated by trained staff, ensure the accurate taking of fingerprints and automatically send the prints to the national fingerprint database. Instead officers take the fingerprints using the old ink method, which can later be scanned into the database. Few officers have much experience of this old process and the results are frequently so poor that they cannot be scanned into the database, although some forces are now providing training on the taking of fingerprints using ink. Technically this is a backward step and also misses the chance for an initial speculative search against the national fingerprint database which

70 Sometimes a decision is made to proceed with the case immediately, for example if the suspect admits the offence and is to be issued with a police caution. In such a case biometrics can be taken straight away.

71 See also Chapter 5 paragraphs 132-133.

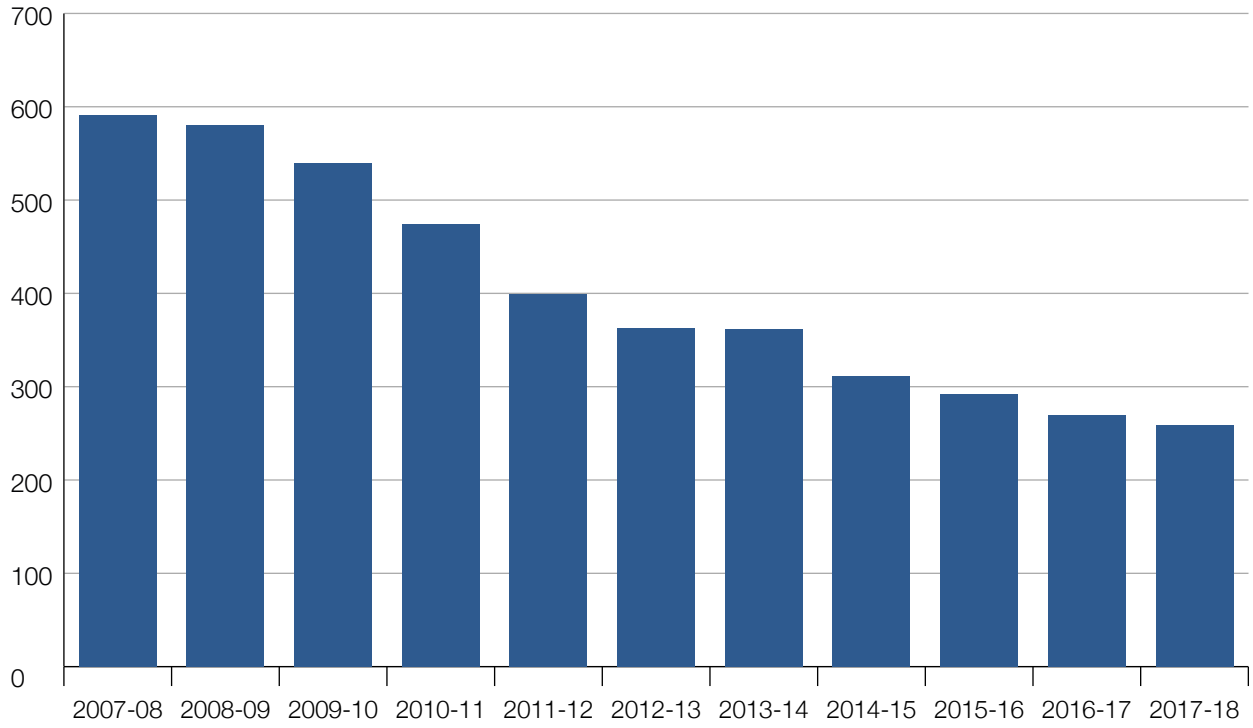
Livescan machines provide. DNA samples can be taken in the same way as in custody suites but, unlike trained custody staff, police officers dealing with VAs will be much less practiced at taking samples and the risk is that error rates will increase.[72]

65. One solution to the lack of facilities for biometric capture outside of custody suites would be to ask VAs to attend a custody suite for the capture of their biometrics. Indeed, this is already requested by some forces. There are though legitimate concerns around bringing someone who has been dealt with under the voluntary attendance process into a custody area to have their biometrics taken, particularly where the subject is very young or is vulnerable. In some cases the decision to keep the subject out of the custody environment has been taken very thoughtfully, so bringing them in later anyway to an extent undoes this work.

66. The overall effect of the growth of the use of voluntary attendance rather than arrest, particularly without clear guidance to forces as to when it is appropriate for a suspect to be a VA or if, when and how they should capture biometrics from VAs, is an inconsistent picture nationally. At the same time there has been a general reduction in the taking of biometrics and therefore in additions to the national biometric databases (this is illustrated particularly starkly in relation to additions of DNA profiles to the NDNAD – see figure 1 below). Even where biometrics are taken there may well be DNA sampling errors and/or fingerprint sets that are of too poor quality for loading or matching purposes. The purpose of having national databases of both convicted offenders and unsolved crime scene stains against which a suspect's biometrics may be speculatively searched will therefore decline in value. This is a fundamental threat to the police use of biometrics for investigative purposes. We have already heard from forces of cases in which a large amount of time and money has been spent on an investigation to identify the perpetrator of a serious crime, only for it to be discovered that the suspect had come to previous police notice for a minor offence and been dealt with as a VA, with no biometrics taken.

72 I have limited this discussion to the biometrics governed by PoFA (fingerprints and DNA) however the same points can also be made about the taking of custody images, especially outside of custody suites.

FIGURE 1: Number of subject profile records loaded onto NDNAD per year (in thousands) (2007/08 – 2017/18)



Source: National DNA Database Strategy Board Annual Report 2017/18

67. There are possible counter measures to these risks. Some forces, such as Greater Manchester Police, are introducing procedures to rigorously chase up the taking of biometrics from VAs, some are training all officers in taking biometrics and forces could put Livescan machines and photo booths in all police stations or develop technology for smaller, more mobile machines for taking fingerprints but these measures will come at a significant cost at a time when policing budgets are limited. Alternatively, Ministers and ultimately Parliament could examine whether there should be a change as to when the police have the power to take biometrics, but this would require legislation and would inevitably raise questions around the necessity and proportionality of such a power.

BAIL AND 'RELEASED UNDER INVESTIGATION'

68. The introduction of the overriding presumption of release without pre-charge bail (unless strict necessity and proportionality criteria are met) has changed fundamentally the way in which suspects are released from police custody. When the changes first came into effect in April 2017 the numbers of suspects being released on bail were reduced to almost zero, such was not only the police perception of the legislative change but the messaging from the Home Office that came with it. Since that time the numbers released on pre-charge bail have increased to around 10% in the forces who have been able to provide me with the relevant data, with the remainder of suspects who are still under investigation (i.e. the vast majority) being 'released under investigation' (RUI).

69. There was a great deal of publicity surrounding the legislative changes made to the rules around bail, following some high-profile cases in which public figures had complained of spending long periods on pre-charge bail. The Home Office issued a press release on the day that the changes came into force stating: "The government today brings an end to the injustice

of people being left to languish on very lengthy periods of pre-charge bail, by introducing a limit of 28 days. The limit is one of several measures taking effect today introduced through the Policing and Crime Act 2017 which will rebalance the police's use of bail in the interests of fairness"[73]. The Home Office did not, however, issue comprehensive guidance to police forces around how they might interpret the new rules or how they would be expected to implement them operationally. Nor do the Home Office appear to have made any assessment of whether, in practice, the police would actually be able to implement the changes or what the effect of the changes would be on police operations. Neither did such guidance come from the centre of policing, for example from the NPCC[74]. As is so often the case, individual police forces were left to work out what the implications of the changes would be and how they should implement them.

70. I wrote to all police forces in April 2017 expressing my concern that cases where suspects were released under investigation would not be monitored as rigorously as cases where the suspect was released on pre-charge bail. This is because in bail cases there are strict deadlines that must be adhered to but for RUIs there are not. I feared that cases would be left to 'drift' and/or that suspects would not be informed of the outcome of the investigation for a protracted period. Unfortunately, my fears have come to fruition, with serious (unintended) consequences for biometric retention. In particular:

(i) When I visit police forces I ask them for data about the number of suspects 'released under investigation' and the time for which they have been under investigation. Some forces are not able to provide this data as they have no way of centrally monitoring these cases. This is indicative of the major problem faced by most forces from the outset; that their IT systems were not able to be quickly (if at all) adapted to record and monitor suspects released otherwise than on bail. Even where IT systems allow cases to be monitored, there have frequently been no processes in place to carry out the required monitoring, so cases that are not a priority are allowed to drift and the suspect remains 'under investigation'. This is now improving, with new procedures being put in place in many forces (sometimes in response to a recommendation from my Office), but this has taken almost two years. The result is that arrestees are often spending longer 'released under investigation' than they were on pre-charge bail. This can mean that biometrics are held for long periods in cases where the result might be eventually be to take no further action (NFA) against the suspect. Given that if the person has no other convictions the biometrics must usually be deleted at this point, biometrics have often been kept for far longer than necessary while the investigation has been ongoing but inactive.

73 https://www.gov.uk/government/news/28-day-pre-charge-bail-limit-comes-into-force
74 I am given to understand that such guidance has recently been issued but I am yet to have sight of it.

(ii) A significant number of forces have reported to me that whilst if they make a decision to NFA a case where the suspect has been released on pre-charge bail their IT systems ensure that the biometrics are automatically deleted (where appropriate) this is not the case for those being dealt with as RUIs, because their systems have not yet been modified to ensure that the result of the case is updated onto the Police National Computer (PNC). In these circumstances the biometrics of RUIs continue to be held unlawfully and could produce unlawful matches. It appears that this problem was not initially identified, with some forces developing large backlogs of cases, running into the tens of thousands where the conclusion of cases has not been updated onto the PNC. I am informed that forces are working, using manual workarounds, to clear these backlogs but in several notable cases have not yet done so[75]. In the meantime, there remain unlawfully retained biometrics. No doubt policing systems will be modified to ensure that these backlogs do not recur in the future, but the costs involved mean that this will not necessarily happen quickly.

71. The government's stated aim upon making the legislative change to pre-charge bail was to reduce the time arrestees spent on bail and stop "the injustice of people being left to languish on very lengthy periods of pre-charge bail". From my observations and discussions with police forces it would appear that in some respects the problem has simply been passed to those 'released under investigation'. Further, suspects may remain RUI for longer than they would have been on bail under the old system. Even when the investigation comes to an end, their biometrics may then be retained unlawfully.

OTHER ISSUES REQUIRING GUIDANCE

72. As discussed in detail elsewhere in this report[76] there remains a further issue in relation to the conflict between PoFA, which requires, put simply, that all DNA samples be destroyed after a maximum of six months and the 'CPIA exception'[77] which in limited circumstances allows DNA samples to be retained beyond six months. Since 2014 both I and my predecessor have highlighted this conflict and our concern that, at least for some police forces in England and Wales, routine and/or 'blanket' retention of large numbers of DNA samples under CPIA had become the norm. As such very real questions have arisen as to whether Parliamentary intention that DNA samples be routinely destroyed was/is being circumvented. It is therefore vital that forces be provided with specific guidance as to how to interpret and apply the exception. In the absence of such guidance I wrote to forces in 2017[78] outlining key principles in respect of the operation of the CPIA exception that forces may wish to consider adopting. I have been inspecting forces this year against those principles and have found the situation to be improving. Unfortunately, the required national guidance has still not been issued by the Home Office or by the police.

75 I am informed for example, by the Metropolitan Police Service, that there are currently 40,000 open cases on the PNC which need to be updated.

76 See also Chapter 6 paragraphs 155-165.

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

78 *Commissioner for the Retention and Use of Biometric Material*, Annual Report 2017, Appendix D

73. It is apparent that issues will continue to come up which need to be carefully considered in terms of whether biometrics can be captured and retained, or whether PoFA covers the specific circumstances that have now arisen. For example, I was recently approached by one police force who wanted to carry out an experimental trial of 'deferred prosecution' (contingent on the suspect admitting the offence and completing a specific programme) for a small number of juvenile offenders who had been interviewed voluntarily. In the usual course of events there is a power to take biometrics from these individuals at the point at which they are charged (i.e. the prosecution is to proceed) but if this is deferred it appears there is no such power to take biometrics. I referred this matter to the Home Office for guidance and this will now be considered by the FINDS Strategy Board. In the meantime, however, in the absence of guidance on this point the experimental trial will not go ahead, which may well be a lost opportunity. Either the issuing of guidance on these types of issues needs to be quicker or the Home Office needs to issue general guidance on the police conduct of experimental trials.

74. One aspect of the section 63G application process that was introduced by PoFA[79], to which my predecessor drew attention and I have pursued, is the general policy necessarily adopted by my Office and the police to address correspondence only to the subject of an application (including children and young people[80]) unless and until they expressly authorise us to do otherwise, due to concerns about privacy and sensitivity of personal information. In practice, however, 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. The obvious answer to this problem would be to seek permission from the young person at the time of their arrest to inform a parent or guardian of any subsequent application to the Commissioner (or indeed to send them any other future correspondence including from the police), unless there are strong reasons not to do so.

75. In December 2016, I discussed the problem with Chief Constable Olivia Pinkney, the NPCC lead on the policing of children and young people. She agreed that the current practice is not satisfactory and undertook to work towards a revised procedure on behalf of the NPCC. Over a year later, at the time of my 2017 Report, the matter had unfortunately not been progressed. During 2018 I was made aware that this work had been passed to ACRO and I was assured of an imminent resolution, including a new practical procedure and associated guidance to forces. I am now informed, however, that the work has been passed to the FINDS Strategy Board, who are due to consider it in April 2019 and there are still no firm plans in place to implement the required procedural changes and guidance. The situation regarding writing to minors therefore remains unsatisfactory, despite this having been raised shortly after the implementation of PoFA, and despite the NPCC, the Home Office and, in this example, ACRO, having been made aware of the problem. This is a serious safeguarding issue as well as one of giving children and young people a fair opportunity to be represented. Further, it is perhaps the worst example I have come across of an issue that has arisen as a result of new legislation being passed around various bodies without anyone appearing to take responsibility and without the required changes being made and/or guidance being produced

79 For more details of which see Chapter 8 of this Report.
80 *Commissioner for the Retention and Use of Biometric Material*, Annual Report 2017, paragraphs 151-156.

76. I am aware of the aforementioned examples of the unintended consequences of changes in policing because they involve the capture or retention of biometrics. I do not know if there are other examples of which I am unaware because they do not involve biometrics[81]. The key question, however, is whether such consequences are inevitable or could be avoided? There are some things that the Home Office might be expected to do before issuing new codes or legislating. For example, it should be possible to identify in advance practical problems such as changing IT systems or modifying police procedures if the police were more involved in the process at an early stage; Home Office specialists could model the likely consequences of changes before they are implemented and build in the time and resources needed for the police to make the necessary changes and comply with any new rules, when considering the legislative schedule. Further, the Home Office and police could work together more closely to ensure that the police have clear, pragmatic guidance as to the meaning of new legislation and associated codes, as well as how it is envisaged that they will be implemented practically. I am aware that such additional considerations would make things more complicated and lengthy for policy makers and legislators, but they would also make it more likely that the intended outcome of legislative change would be achieved. The current state of affairs means that after any significant change there can be a significant period of confusion, often followed by non-compliance and a number of unintended, potentially damaging consequences.

81 I am, however, acutely aware of the forensic science market instability that has arisen over the last two years, as a result of earlier changes to the provision of forensic science services to the police. See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786137/FSRAnnual_Report_2018_v1.0.pdf

4. BIOMETRICS AND NATIONAL SECURITY

COUNTER TERRORISM POLICING AND POFA

77. Counter-terrorism policing in the UK consists of regional Counter-Terrorism Units (CTUs) based in England, Wales and Scotland, coordinated by the Metropolitan Police Service's Counter-Terrorism Command (SO15) and in Northern Ireland by the Police Service of Northern Ireland (PSNI). My job as regards NSDs is laid down in PoFA and is to keep under review:

(i) every NSD made or renewed; and

(ii) the uses to which the biometric material retained is being put.

78. NSDs are made by Chief Officers of police but if I do not think that retention of the relevant material is necessary or proportionate then I have the power to order its destruction.[82] This is a significant power which, given the threats being managed, I should exercise carefully and I do not take such a decision without first challenging the original decision to ensure that I am aware of all the matters taken into account by the Chief Officer and their reasons for making an NSD.

79. 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 any holdings by non-law enforcement agencies, such as the security and intelligence services or the military. Law enforcement bodies for these purposes are defined in PoFA[83] and have access to the various police biometrics databases.

80. My responsibility, as Biometrics Commissioner, is to report to the Home Secretary on compliance with the legislative requirements that apply to counter terrorism policing. I am aware that my insistence on raising this issue of compliance must sometimes seem irksome to the Counter-Terrorism Command. The Command has the difficult job of keeping the country safe from the threat of terrorism and focusing on governance and legality can easily seem diversionary from the action orientation required. I should therefore record the courtesy and acceptance with which the Command has responded to my requests. It would be all too easy to side-line issues of legality and governance on grounds of the greater good of achieving results. That the Command has not done so does them great credit.

POLICE BIOMETRICS AND NATIONAL SECURITY DETERMINATIONS

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

82 PoFA sections 20 (2) (a & b), (4) and (5).
83 See Parts I to VII of Schedule 1 of PoFA.

82. A responsible Chief Officer or Chief Constable[84] has the power under PoFA to order that such biometrics should be retained on grounds of national security. They may only do so by agreeing to a National Security Determination or 'NSD'. The power to make an NSD applies across the UK and is not limited to England and Wales because national security matters, unlike criminal matters, are not devolved.

83. An NSD must be in writing and lasts for a maximum of two years beginning with the date it is made.[85] An NSD may be renewed for a further period of two years and can be considered for renewal on any number of further occasions. For further details of these provisions see Appendix C.

LEGISLATIVE CHANGES AFFECTING NSDS

84. Following the terrorist attacks that took place in the UK in 2017 the Prime Minister promised to bring forward further counter-terrorism legislation. The legislation – the Counter-Terrorism and Border Security Act 2019 – received Royal Assent on 12 February 2019. The biometric provisions have not yet come into force as the Home Office has to take guidance through Parliament and the police will need some time to make the necessary changes to their processes and IT systems. It is likely that they will come into force in the latter part of this year. The Act makes some changes to the police retention and use of biometrics for counter-terrorism purposes.

85. Under the new legislation Chief Officers continue to have the power to make NSDs but they will now last for a maximum of five rather than two years. I have been broadly supportive of this change because in some cases it may be reasonable to assess that the risk presented by an individual is not only significant but also likely to continue for some time and in such cases a five year NSD will be appropriate. In other cases, the risk being assessed for an NSD may be evidenced enough to justify retaining the subject's biometrics but not yet certain or clear enough to justify a five year retention. Even under the current legislation a Chief Officer would occasionally find that whilst making an NSD was necessary and proportionate there was sufficient uncertainty going forward that either the case should be reviewed before the two year period was completed or that if the case came up for renewal then further information would be needed to justify a renewal. The new Act does say that an NSD can be made for a *maximum* of five years, as PoFA had done for the two year maximum NSD period. However, I am not aware of any NSD that was cancelled before the two year retention was completed. Perhaps with a two year maximum and given the time taken to assemble the evidence either to make or review an NSD this was inevitable. However, with the new five year maximum it is reasonable to expect the police to have a process in place that enables them both to identify suitable cases and to review them at appropriate intervals before the maximum period is completed. I have already indicated to the Counter-Terrorism Command and the Home Office that I wish to discuss this issue with them before the new legislation comes into force and I shall report on that in my next report.

86. Under previous legislation the police had the power to automatically retain the biometrics of those arrested on suspicion of terrorist offences for three years, but only if the individual was arrested under the Terrorism Act 2000 (TACT). However, for other arrests on suspicion of terrorist offences they did not have this power, if the individual was arrested under the

84 (i.e. the Chief Officer or Chief Constable of the force or authority that 'owns' the biometric records at issue).
85 The statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different (see further Appendix C).

standard power of arrest in PACE.[86] I commented that this seemed to me to be an anomaly. The new legislation brings the rules applying to the retention of biometric data of persons arrested for terrorism offences under PACE into line with those applying to persons arrested for the same offences under TACT.

87. I also commented in previous Reports that some NSDs were being approved by Chief Officers before there was clear evidence as to their necessity. These were usually cases where the individual had been arrested and either an investigation had been started but not completed or, more rarely, a charge had been made but the legal process was not yet complete. This was what I referred to as 'pre-emptive NSDs'; because there was no need for an application since in either case the police could retain the biometrics at least until the investigative or legal processes were complete. The police reason for doing so was because if they decided to take no further action in an investigation and there was no other lawful basis for retaining the biometrics they would be almost immediately destroyed. Where there had been a charge, but the prosecution did not proceed or the trial resulted in an acquittal, then the biometrics would have to be destroyed without there being time to consider an NSD if there was no other lawful basis for retaining them and the charge was not for a qualifying offence. I continued to express my unhappiness with this situation, especially because I saw no evidence that these pre-emptive NSDs were re-visited once the investigative or legal processes were complete. I agreed in the short term not to use the power afforded to me under s20(4) of PoFA to order the destruction of the material, but only until the Home Office had completed the new legislation.

88. The new power to retain for three years the biometrics of all those arrested on suspicion of a terrorist offence should eliminate the need for many of these pre-emptive NSDs, but I will monitor the situation closely. The police may continue to try and use pre-emptive NSDs for yet to be completed investigations for non-terrorism related offences or charges for non-terrorism related/non-qualifying offences but where the individual is still considered to be a threat to national security. The same problem could have arisen in relation to general crime, but in that case the Home Office issued guidance which gives the police 28 days to consider other action (such as an application to me under s63G of PACE) before the biometrics are deleted[87]. As I understand it the Home Office could issue similar guidance, allowing a reasonable time period for the police to complete all of the processes needed to make an NSD, to be followed in cases where an individual is arrested for a non-terrorism related offence (and a decision is made to take no further action) but is nevertheless thought to pose a threat to national security. I have suggested to the Home Office previously that such guidance should be issued but now that the new CT legislation has been passed I urge them to do so as part of the guidance and so remove the need for any pre-emptive NSDs. If they do not do so and the police continue to make pre-emptive NSDs then I will feel compelled to consider exercising my power to order the biometrics to be destroyed where there is no other legal basis to retain them.

89. Under PoFA an NSD could only be granted by a Chief Officer of the force where the biometric data was taken. This meant that some Chief Officers in forces where NSDs were regularly considered (such as at the MPS Counter-Terrorism Command or those forces covering a major airport or port) were experienced at making the necessary judgements. In some other forces NSDs were very rarely considered and the Chief Officers had little experience of such

86 Because the longer period of pre-charge detention and other exceptional powers available following arrest under TACT (on suspicion of being a terrorist) were not necessary.

87 In practical terms the police must decide within 14 days whether to make an application and place an appropriate marker on the PNC to stop the biometrics from being automatically deleted, which if no marker is in place, happens 14 days after a decision to take no further action is recorded on PNC.

judgements or of the wider national security context. I commented in last year's Report that I had observed this to be resulting in some inconsistency of decision making. In such cases I have been challenging the decisions that either I do not consider to have been properly justified as necessary and proportionate, or were out of line with the generality of decisions, to try and ensure that NSDs were properly decided by all Chief Officers and a more consistent process followed. The new Act has replaced the requirement that the Chief Officer deciding an NSD must be from the force taking the biometric data, with a requirement simply that a Chief Officer must make the decision. I understand that the police intend that each Regional Counter-Terrorism Unit should have a designated Chief Officer or Officers who will consider NSDs. This should mean that NSDs will all be considered by a smaller group of Chief Officers who are also more experienced at doing so and who will have knowledge of and the context around the threat posed by the individual being considered. That should deal with the problem of inconsistent decision making and in that regard I welcome the change. By the same token, however, there is always a risk that such a group will fall prey to what psychologists refer to as 'confirmation bias' and I will be alert to such a risk in carrying out my obligation to review all NSDs.

90. Finally, PoFA required that NSDs had to be made in respect of biometric material, rather than for the person to which the material relates. This meant that each time a new DNA sample and/or set of fingerprints was taken for an individual, a new NSD should have been made in order to retain those biometric records. The new CT legislation changes this, by making an NSD in respect of the person rather than the material retained. This is a sensible change since the risk being managed relates to a person

COMPLIANCE WITH POFA

91. In previous Reports I have commented that that as far as compliance with those elements of the Police and Criminal Evidence Act 1984 as modified by PoFA is concerned the police are generally compliant and all police forces, despite specific areas of concern, are making considerable efforts to be compliant. The situation as regards compliance with the counter-terrorism provisions of PoFA has been less favourable, largely due to the Counter-Terrorism Command failing to bring their legacy holdings of biometric material into compliance with the requirements of PoFA.

SECTION 18 COUNTER-TERRORISM ACT 2008

92. I explained last year that the Counter-Terrorism Command had failed to bring their holdings of biometric material received from foreign law enforcement bodies or other UK agencies into line with the requirements of section 18 of the Counter Terrorism Act 2008 (CTA). That Act requires that where such material is received it may be retained in the first instance for three years but thereafter only if it either has been received without any biographical identifiers or has been awarded an NSD.

93. I reported in detail on this issue last year and that the Counter-Terrorism Command, having reviewed the almost one million such biometrics had concluded that only 173 of those holdings that were not anonymous (i.e. they could be identified to an individual) did they judge needed to be retained for national security purposes. This could have been achieved by a Chief Officer making an NSD for each case. However, the Metropolitan Police received legal advice that they could make group NSDs rather than making an individual NSD for each case. I was surprised by this advice and therefore took my own independent legal advice which came to

the conclusion that a group NSD appears to be permitted according to the wording of the relevant legislation but that the tests of necessity and proportionality needed to be met for each individual included in the group.[88]

94. In the event the police made four group NSDs to cover the 173 individual cases and I was satisfied that each NSD contained evidence to justify the inclusion of each individual within the group. Having been satisfied on that basis as to the evidence justifying the necessity and proportionality for each individual in each NSD and in the light of my legal advice I did not challenge the four group NSDs. Ironically, in the event the group NSDs contained information pertaining to each individual that could have been the basis for individual NSDs.[89] The police have not suggested any further use of group NSDs and I shall be concerned if they were to do so outside the unusual situation created by bringing their holdings into line with the section 18 requirements. I am grateful for the cooperative way in which the Counter-Terrorism Command and the MPS's Forensic Services kept me informed on this matter.[90]

GOVERNANCE

95. Previous Reports have commented on a 'governance deficit' as regards the comprehensive governance arrangements and protocols that might be reasonably expected of CT policing.[91] This year FIND-SB have added the CT biometric databases to their governance where they will be dealt with in the same way as other police DNA and fingerprint database holdings. This is a significant step in improving the governance of the CT databases and essential as the new HOB data platforms come into use. In addition, this year the Counter-Terrorism Command has introduced direct reporting by the PoFA CT Programme Board to the National Security Biometrics Board, which is chaired by the Commander of Counter Terrorism. This is a higher level of accountability than applied in the past and I hope will prevent the problems previously experienced. The Counter-Terrorism Command have agreed that I have oversight of this new governance structure, including attendance by myself or a member of my staff at each of these Boards and I grateful to them for doing so.

MOD SEARCHING INTO THE POLICE NATIONAL FINGERPRINT DATABASE

96. Within the national fingerprint database (IDENT1) there are a number of separate police collections of fingerprints. For example, there is the Police National Fingerprint Database (PNFDB) but also a separate Police Counter-Terrorism Database. When IDENT1 was created it was purely used for police fingerprint databases. However, when the military started collecting fingerprints during their operations that meant that they needed a fingerprint database. The Ministry of Defence (MoD) was therefore given permission in 2012 to have their own, separate,

88 Taking such advice was problematic because there is no provision in the budget for the Office of the Biometrics Commissioner (OBC) for the taking of independent legal advice and there is no other route for taking such advice. In this case it was possible because earlier understaffing of the OBC meant that money was available to pay for the advice. That would not be the case in the future yet legal advice might be necessary and I am in the process of seeking assurances from the Home Office that there is some contingency outside of my budget to pay for such advice if it were needed.

89 On this see the note added to the OBC website at the time – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715866/2017_Annual_Report_Update.pdf

90 I reported last year that the deletion of the unlawful holding was in progress. Unfortunately, I have recently been informed that 275,000 biometric records are being held unlawfully (albeit in an unsearchable format) due to administrative and new governance issues put in place to avoid the inadvertent deletion of legally held material. The police and Home Office have assured me that they are working to rectify this as soon as possible.

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

cache of fingerprints within IDENT1. This cache is the only non-police collection within IDENT1. Hosting the MoD cache within IDENT1 was deemed a cost-effective solution since the IDENT1 system was already operational and commercially proven.

97. I reported last year that the MoD wanted to check whether fingerprints taken or found during military operations abroad matched to persons known to the UK police or immigration authorities or matched crime scene fingerprints held by the police. In order to perform these checks a search must be made against all of the police's fingerprint collections. It seems to me to be in the public interest that such searches should be possible, to support military operations abroad and counter-terrorism operations at home. However, such inter-departmental searching of biometric records should have a lawful basis and agreed governance arrangements[92].

98. PoFA made available a route by which such checks could be made and put in place a set of rules for the retention and use of DNA and fingerprints by the police and other law enforcement agencies which are specified in the legislation. The MoD police and the other military police are listed as law enforcement agencies who can ask for searches against the PNFDB through the powers laid down in the PACE (Armed Forces) Act 2006.[93] However, the MoD have not being searching via the routes permitted by the aforementioned powers but instead the searching is being carried out by the Defence Scientific and Technology Laboratories (Dstl) which is the research and technology arm of the MoD and not a law enforcement agency.

99. Given that the MoD were not using the route available to them under PoFA I have challenged the MoD repeatedly as to the legal basis on which Dstl has gained direct access to and is searching the police's fingerprint collections. I also wrote last year to the Permanent Secretary of the MoD seeking clarification on this issue. Over the last eighteen months the MoD has come up with a series claims as to the legal basis of carrying out their searching through Dstl, none of which I have found convincing. I have also repeatedly pointed out to them that PoFA does provide lawful routes by which the purpose of such searches could be achieved but they have so far declined to follow this route.

100. The PNFDB is under the collective control of the Chief Constables, who are legally responsible for all of the police fingerprint collections on IDENT1. The National Police Chief's Council (NPCC) represents the collective interest of these Chief Officers and was unaware of the Dstl searching into their collections. I suggested to the NPCC that they might consider taking legal advice as to the lawfulness of Dstl carrying out searches into their fingerprint data. This they have now done, and counsel for the police, providing the advice, did not identify any lawful basis for the Dstl searching of the PNFDB. If the Chief Constables allow this situation to continue then they collectively will bear the risks.

101. All parties agree that whilst the searching is in the national interest, a lawful basis for doing so has to be found and implemented urgently. I am disappointed at the time it has taken to reach this point and the failure of the MoD to appreciate the seriousness or the urgency of this situation. The issue has been taken up by the Chair of FIND-SB, ACC Ben Snuggs, and we are now at a point where two possible solutions have been proposed and these are being evaluated and developed by the police, MoD and Home Office. It will need to be clear that either option provides a lawful basis for searching before being put to the NPCC. I hope that

92 There is also a question around quality standards as fingerprint comparisons undertaken by police fingerprint bureaux are expected to meet international standards (particularly ISO 17025), whereas the comparisons being made by the MoD are not inspected to the same standard.

93 As amended by PoFA.

the NPCC will now be able to take a decision on this matter as soon as possible. I shall report as soon as the situation is resolved on the outcome and what I hope will be that this searching has been placed on a lawful footing.

COUNTER-TERRORISM DATABASES

102. Biometrics retained under an NSD are held on separate counter-terrorism DNA and fingerprint databases.[94] All new DNA profiles and tenprint fingerprint sets which are loaded to the NDNAD and IDENT1 are checked against those CT databases.[95]

103. 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 December 2017 was some 11,841 and as at 31 December 2018 was some 11,850. Those latter figures encompass both new additions to the databases since 31 October 2013 and deletions from those databases after that date.

104. Of the individuals whose biometric records were being held by the police on those databases as at 31 December 2018 some 1,994 (i.e. about 17%) had never been convicted of a recordable offence.

TABLE 2: Holdings of biometric material on the CT Databases (year ending 31 December 2018)

		2017	2018
DNA	**DNA**	9,072	8,109
	Of which unconvicted	2,171 (24%)	1,406 (17%)
Fingerprints	**Fingerprints**	9,966	11,168
	Of which unconvicted	1,623 (16%)	1,877 (17%)
Totals	**Total holdings of material**	19,038	19,277
	Of which unconvicted	3,794 (20%)	3,283 (17%)
	Individuals on databases[96]	11,841	11,850
	Of which unconvicted[97]	2,358 (20%)	1,994 (17%)

Source: SOFS

THE NSD PROCESS

105. As explained above, deciding whether an NSD should be approved is a matter for a Chief Officer of police.[98]

94 See *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraph 167, for further details.
95 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.
96 Taking into account those with DNA and fingerprints held
97 Taking into account those with DNA and fingerprints held
98 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.

106. Initially applications to Chief Officers for NSDs are put together either by the MPS Counter-Terrorism Command or PSNI. PSNI deals with all Northern Ireland cases but the MPS oversees all other cases and most of those are signed off by the Counter Terrorism Commander. Applications for retention of biometrics taken in other Counter Terrorism regions are signed off by their respective Chief Officers (see also paragraphs 82 and 89 above).

107. The information upon which applications to make an NSD are based is drawn from police records of previous criminal justice system contacts, domestic police intelligence and EU policing intelligence (if relevant) with additional information from the Security Service, who will provide their holding code[99] as additional supporting information for the NSD decision. After recent terrorist incidents and the report by David Anderson QC[100] the Security Service have re-examined their holding codes to ensure that they better reflect the residual risk of an individual as judged by the Service. Oversight of the Security Service is outside of my remit but we have discussed how their revised holding codes could help Chief Officers decide whether to make an NSD in relation to individuals to whom such codes are attributed. I have further sought reassurance about the extent to which these codes are accurate and can be relied upon, particularly where the only information available about an individual subject to an NSD application is held by the Service. I am grateful to the Security Service for discussing this issue with me.

108. If it is decided that an NSD application should be made, the supporting information is summarised on the application form. A case is also presented as to whether retaining biometrics is necessary on grounds of national security and, if so, whether such retention would be proportionate. The Counter Terrorism Command or PSNI add a reasoned recommendation to the application which also proposes to the Chief Officer whether the supporting intelligence/evidence is adequate to justify making an NSD. The decision is for the Chief Officer, regardless of the advice offered, and they must give reasons for their decisions. There is Statutory Guidance on what should be considered.[101]

109. Dedicated application software is available to all stakeholders in the NSD process. That software runs on the police's National Secure Network to which I have access. If an application for an NSD is approved, the decision of the Chief Officer is recorded at the end of the application together with his or her reasons for approving the application. That document then becomes the NSD and is available to me for my review.

110. Until this year I also received copies of any applications that were refused by Chief Officers so that I could oversee the entirety of the process. This year the Counter-Terrorism Command implemented revised software for NSDs which unintentionally has denied me access to these refused NSDs. I have made clear that this is unacceptable since it prevents me reaching an overall view of how the NSD process is operating. I am assured that a further revision of the software will correct this situation, but I do not know when this will happen. In the meantime, I have had to rely on examining a small sample of these refused NSDs made available to me.

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

100 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

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

111. Notwithstanding this limitation to my oversight, 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 even if, in a small number of cases, after challenge from me. I hope that this latter problem will be dealt with by the new rules on which Chief Officers can agree to NSDs.

112. As can be seen in Table 3, 497 NSDs were made by the Counter-Terrorism Command and PSNI during 2018 (an increase of 54% compared to last year, which can be accounted for by the large number of renewals in addition to new NSDs). I supported 468 of the NSDs made in 2018 and I raised challenges in 55 of the cases I examined. In 11 of these I ordered the destruction of the biometric material since I was not persuaded by the police response to my challenge, to the extent that I could not assess the NSD made as being necessary and proportionate.[102]

TABLE 3: NSD decisions (year ending 31st December 2018)

	2017 (SO15[103] & PSNI)	2018 – SO15[104]	2018 – PSNI[105]
Total possible NSDs applications processed	**1,170**	**1,440**	**40**
Renewal NSDs considered	158	436	12
New NSDs considered	1,012	1,004	28
NSDs approved by Chief Officer	**322**	**488**	**9**
Renewals	77	222	6
New NSDs	245	266	3
NSDs declined by Chief Officer	**27**	**32**	**0**
Renewals	3	15	0
New NSDs	26	17	0
NSDs supported by Commissioner	**325**	**459**[106]	**9**
NSDs challenged or further information sought	34	55	0
Destruction ordered by Commissioner	26	11	0

Source: SO15 and PSNI

113. Most of the challenges I have made have been because either I had doubts as to whether the case presented offered a Security Service holding code that was based on an up to date assessment of the risks that the individual presents (particularly where the decision appeared to have been made mainly based on that code), or whether the Chief Officer had exercised their mind in making the decision and not simply relied on the recommendation presented to them. This latter problem has been associated with Chief Officers new to the NSD process

102 Some NSDs made in late 2018 will have been considered by the Commissioner in early 2019.
103 SO15 (the MPS Counter-Terrorism Command) coordinate all NSDs for England, Wales and Scotland.
104 SO15 (the MPS Counter-Terrorism Command) coordinate all NSDs for England, Wales and Scotland.
105 Small numbers for PSNI are accounted for by the further extension of the PoFA legacy period.
106 Some NSDs made in late 2018 will have been considered by the Commissioner in early 2019.

who have either not been properly briefed or not understood the guidance. I hope that the former problem will be at least reduced by the revised system of holding codes that the Security Service have introduced although I recognise that given the pressures on the Service there may still be some problems as to how current they are. As far as the latter is concerned I hope that the revised rules about which Chief Officers can make NSD decisions will eradicate this problem.

THE USE TO WHICH BIOMETRIC MATERIAL IS PUT

114. I am required to keep under review the process of making NSDs and the use to which retained material is subsequently put. Last year I had to report that because of the continuing PoFA legacy issues in the Counter Terrorism Command I had only been given limited material and so my reporting on the use made of NSD material was very limited.

115. During 2018 the Counter-Terrorism Command and the MPS Secure Operations Forensic Services (SOFS) have been able to provide me with some more data and further narrative about the use to which some of the NSD retained material has been put. However, the detail in the reporting has continued to be hampered by lack of resourcing. As can be seen in Table 4 below the majority of biometric matches against NSDs came about from arrests and further Schedule 7 stops. In three cases a DNA profile held under an NSD was matched to a crime scene stain and in one case fingerprints held under an NSD were matched to a fingerprint taken from a crime scene.

TABLE 4: Matches with NSD retained material (year ending 31 December 2018)

Type of biometric match	Number of matches
Fingerprint Crime Stain to Ten Prints	1
Ten print (Arrestee/Schedule 7 etc) to Ten Prints	72
DNA Crime Stain to DNA Reference Profile	3
DNA Reference Profile to DNA Reference Profile	32
DNA Arrestee to DNA Reference Profile	9

Source: SOFS and SO15

116. A dip sample has been undertaken by the Counter-Terrorism Commend across ten cases in this reporting period, where a newly taken biometric matched to NSD retained material (this equates to 8.5% of all matches). Some of the dip-sampled matches have evidenced the importance of NSDs and the benefit they may have in identifying and apprehending suspects, thus reducing the risk to national security. In one case, the body of a foreign fighter in Iraq was identified from NSD retained fingerprints and in another an asylum application was linked to possible terrorist activity. In the other eight cases dip sampled the match enabled identification and gave an opportunity for the disruption of potential terrorist activity.

117. I appreciate the work done by the Counter-Terrorism Command to provide me with this dip sample but I hope that the new software they are introducing later this year will enable routine tracking of the use made of NSDs that is clearly of as of much interest to their management of the terrorism risk as it is to my oversight role.

CASES REVIEWED AND NSDS MADE

118. During 2018 the cases of approximately 1,480 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 the Counter-Terrorism Command /PSNI for NSD purposes (see Table 3 above).[107]

NSDS IN NORTHERN IRELAND

119. The only assurance role that I fulfil in Northern Ireland is in relation to counter-terrorism holdings and the granting of National Security Determinations, since in this regard I have UK-wide responsibility.

120. The Police Service of Northern Ireland Legacy Investigations Branch and Police Ombudsman has responsibility to investigate deaths in Northern Ireland related to the historic conflict in Northern Ireland. In June 2016, a Statutory Instrument was laid before Parliament by the Northern Ireland Office amending the existing Transitional Order and thereby extending the PoFA Legacy period in Northern Ireland for a further two years, until 31 October 2018[108] and was repeated again in 2018, until 31 October 2020.[109] This Order applies only to Northern Ireland biometric material taken under counter-terrorism powers before 31 October 2013 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"*.[110]

121. The upshot of this amendment is that generally national security Legacy cases in Northern Ireland will no longer be reviewed as to PoFA compliance until after 31 October 2020. However, unless a further such a Statutory Instrument is passed by Parliament, then PSNI must either consider legacy material for an NSD or delete it by that date. At present it is difficult to comment on when Northern Ireland will implement the counter-terrorism provisions of PoFA insofar as it relates to legacy material since as I write there has been no significant progress on draft legislation to address the legacy of the past in Northern Ireland.

122. New biometrics taken in Northern Ireland as part of a national security investigation under the Terrorism Act 2000 (TACT) since the commencement of PoFA on 31 October 2013 must be treated in the same manner as elsewhere in the UK and be fully PoFA compliant. PSNI are fully compliant in relation to material taken under counter-terrorism powers since the commencement of PoFA.

123. I am informed by PSNI that to date there has been one biometric match of a crime scene mark against material held under NSDs agreed in Northern Ireland, with three further subjects of NSDs now suspects in current investigations. This is based on searches of the material against both local and national fingerprint and DNA databases. It must be noted, however, that NSDs made by PSNI represent only a small proportion of the total number of national

107 Special thanks to staff within SO15, SOFS and PSNI for their help in compiling the relevant data and more generally for their assistance during the 2018 reporting year.
108 http://www.legislation.gov.uk/uksi/2016/682/contents/made
109 http://www.legislation.gov.uk/uksi/2018/657/contents/made
110 http://www.publications.parliament.uk/pa/ld201617/ldselect/ldsecleg/25/2504.htm

security holdings as they are only made in relation to new biometric material, due to the legacy arrangements outlined above[111].

DATA LOSES

124. Previous annual reports have recorded that a number of IT issues, procedural and handling errors have led to the loss of a significant number of new biometric records that could and should have been retained on the grounds of national security. During 2017 most of these issues appeared to have been resolved, with the new biometrics of 13 additional individuals lost; a substantial improvement on previous years. It is therefore disappointing to report that during 2018 the new biometrics of 144 additional individuals have been lost. As can be seen in Table 5 below, 104 of these losses were a result of an administrative error made during a manual data transfer to the software application used to manage NSDs. Eight cases were not reviewed by Chief Officers before the relevant biometrics reached their statutory deletion date, so the NSD could not be made. Eight cases were not progressed on time by the Counter-Terrorism Command. The remaining 24 losses were recorded as lost by MPS forensic services as the result of an oversight in notification after the Schedule 7 stop had taken place. I am informed by the Counter-Terrorism Command that of the 144 losses of biometric material, it is estimated that in 125 cases the material would not have been considered for retention under an NSD. In the remaining 19 cases, where there were concerns that the individual to whom the lost biometric material belonged may have posed a threat to national security, necessary steps have been taken to assess the necessity and proportionality of re-acquiring the lost biometric material.

TABLE 5: Losses of biometric material of potential CT interest (year ending 31 December 2018)

Reason for loss of biometric data	Number of losses of biometric material
Administrative error by SO15	104
Case not reviewed by Chief Officer within statutory time limit	8
Case not progressed within statutory time limit	8
Taking of material not notified to SOFS	24
Total	144

Source: SO15

125. I am further informed that the Counter Terrorism Command have now taken steps to minimise the loss of biometric material, in particular through administrative errors, in future. A dedicated unit was set up in early 2018 to process potential NSDs and that unit are responsible for carrying out new quality assurance checks. In the longer term, the MPS have been working on implementing a new IT system, with a single software solution to minimise manual inputting and improve the accuracy and efficiency of data management and review of applications. Whilst I acknowledge that time and resources are needed to implement such a solution it is concerning that over five years after the implementation of PoFA such errors, with a potential risk to national security, are still being made.

111 Before the extension was agreed PSNI made NSDs in relation to a small number of legacy cases. These still stand and must be/have been renewed where appropriate for the material to continue to be retained.

5. BIOMETRIC RETENTION AND USE

THE GOVERNANCE OF NATIONAL DATABASES

126. The National DNA Database (NDNAD) was overseen by the National DNA Strategy Board (NDNASB), which was given a statutory role in PoFA.[112] In March 2016, fingerprints were added to the remit of the Board and it has become the Forensic Information National Databases Strategy Board (FIND-SB). FIND-SB monitors the performance of these databases and their use by the police. It also issues guidance to the police on the use of the databases, including in relation to meeting the requirements of PoFA. In 2018 it was agreed in principle that FIND-SB would be best placed to take responsibility for the oversight of the processes involved in the UK joining the Prüm exchange.

127. The extension of the remit of the Strategy Board was a welcome development since it brought DNA, fingerprints and the counter-terrorism databases (all subject to regulation by PoFA) within a proper, transparent and, moreover, mature national governance structure. Adding oversight of Prüm also is sensible since it avoids different uses of DNA and fingerprints being subject to different Home Office governance processes. There are, however, other police biometric databases that are not within the remit of FIND-SB, most notably the facial images held on the Police National Database (PND). In its Biometrics Strategy[113], which was published in June 2018, the Home Office committed to 'develop options to simplify and extend governance and oversight of biometrics across the Home Office sector through consultation with stakeholders over the next 12 months'. This is a welcome development.

128. FIND-SB is chaired by a representative of the National Police Chiefs' Council (NPCC), currently ACC Ben Snuggs, and includes representatives of the Home Office and of the Police and Crime Commissioners who are the voting members. Also in attendance as observers are the Chair of the Biometrics and Forensic Ethics Group,[114] the Forensic Science Regulator, the Biometrics Commissioner, the Information Commissioner[115] and representatives of the devolved administrations.

129. FIND-SB publishes an annual report which is laid before Parliament[116] and includes data about the operation of the databases. Some similar data is included in this report simply to ensure that it is self contained for the reader, although our data is mainly for a calendar year rather than a fiscal year as in the FIND-SB Report.

NATIONAL DNA DATABASE

130. The National DNA Database was established in 1995 and, by the end of the calendar year 2018, held 5,780,239 subject DNA profiles for England and Wales. This equates to an estimated 4,991,536 individuals. UK holdings total 6,957,359 subject and crime scene profiles or an estimated 5,461,561 individuals. The number of DNA subject profiles added to the database has declined. This is as a result of a reduction of new individual profiles being added to the

112 See section 63AB of Police and Criminal Evidence Act 1984 (PACE) as inserted by section 24 of POFA.
113 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf
114 Originally called The National DNA Database Ethics Group, during 2017 it was given an extended remit to match that of the Strategy Board and re-named the Biometrics and Forensic Ethics Group – see https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group
115 See http://www.ico.org.uk/
116 https://www.gov.uk/government/publications/national-dna-database-annual-report-2017-to-2018

database because of a reduction in the number of arrests which generally is the lawful basis for the taking of biometrics (see Chapter 3). The numbers have declined from 540,100 profiles added in 2009/10 to 256,422 in 2018[117].

TABLE 6: Number of DNA profiles held (year ending 31 December 2018)

	Subject Profiles	Crime Scene Profiles	Total
England and Wales[118]	5,780,239	588,557	6,368,796
Rest of UK[119]	561,002	27,561	588,563
Total	**6,341,241**	**616,118**	**6,957,359**

Source: Data supplied by FINDS-DNA[120].

TABLE 7: Total DNA Holdings on NDNAD by Profile Type (year ending 31 December 2018)

	Arrestee	Volunteer[121]	Crime-scene from mixtures[122]	Crime-scene from non-mixtures	Un-matched crime scenes[123]
England and Wales	5,778,225	2,014	102,253	486,304	188,613
Rest of UK	558,813	2,189	1,851	25,710	17,225
Total	6,337,038	4,203	104,104	512,014	205,838

Source: FINDS-DNA

131. The significant increase in crime scene stains involving mixtures of more than one person's DNA (up from 80,270 in 2017 to 104,104 in 2018) reflects the increasing ability of forensic scientists to analyse such complex stains.

NATIONAL FINGERPRINT DATABASE

132. The National Fingerprint Database became fully operational in 2001 and held all fingerprint sets (tenprints) taken from persons arrested in England and Wales and those from Scotland and Northern Ireland convicted of certain serious offences. The present IDENT1 system came in to use in 2004 and also enabled the storage and search of arrestee palm prints and unidentified palm marks from scenes of crime. In 2007 Scotland began enrolling tenprints obtained for arrests in Scotland to IDENT1 and Northern Ireland in 2013. Presently, fingerprints taken under PACE or its equivalent in the UK are enrolled onto IDENT1 for storage and search.

117 Previous figures were for fiscal year. This is now given for the calendar year in line with the rest of this Report. The comparable figure for fiscal year 2017/18 is 259,099 new subject profile records were loaded to NDNAD. All figures for fiscal year are sourced from the FIND-SB Annual Report 2017/18.
118 Includes British Transport Police.
119 Includes Scotland, Northern Ireland, Channel Islands, military police forces and Customs and Excise.
120 Special thanks to Kirsty Faulkner and Caroline Goryll of FINDS-DNA for their help in preparing the relevant data.
121 '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.
122 Mixed profiles include the DNA information of two or more persons.
123 The number of unmatched crime scenes is included in the crime scene from mixtures and non-mixtures figures.

133. The present Livescan[124] system for the automatic taking and searching of prints came into operation in 2002 and has recently been updated as part of the Home Office's Biometrics Programme (HOB).

TABLE 8: Total Holdings on IDENT1 by classification (year ending 31 December 2018)[125]

	Tenprint sets from arrestees	Number of individuals with prints on IDENT1	Unmatched crime scene marks	Number of cases with unidentified crime scene marks
England and Wales	24,053,339	Data not available	1,944,475	Data not available
Rest of UK	1,127,478	Data not available	320,435	Data not available
Foreign convictions	Data not available	Data not available	Data not available	Data not available
Total	25,180,817	8,203,873	2,264,910	955,650

Source: FINDS – National Fingerprint Office in consultation with IDENT1 supplier

THE USE OF DATABASES

Additions to NDNAD in 2018

134. The National DNA Database as of the year ending 31 December 2018, held 6,341,241 subject profile records and 616,118 crime scene profile records. In 2018, 256,422 new subject profiles were added to the database, and 37,487 crime scene profiles were also added to the database (See Table 9 below).

TABLE 9: Additions to NDNAD (year ending 31 December 2018)

	Arrestee	Volunteer[126]	Crime-scene from mixtures[127]	Crime-scene from non-mixtures
England and Wales	227,462	3	24,877	10,945
Rest of UK	28,938	19	469	1,196
Total	256,400	22	25,346	12,141

Source: FINDS-DNA

124 Livescan is an electronic fingerprint capture system for capturing subject fingerprint and palm print data for enrolment onto the database
125 The data in this table is comparable to the data in the 2017 Report Table 3 and Table 4: Arrestee Tenprint Fingerprints and number of cases with unidentified crime marks. It originates from the same source as the 2017 data.
126 '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.
127 Mixed profiles include the DNA information of two or more persons.

135. The number of profiles held on the National DNA Database reached a peak of 6.97 million in the **fiscal** year 2011/12, declined to 5.63 million in 2012/13[128] and then increased to its present level of 6.34[129] million; this is in large part because the number of new profiles loaded has declined from 540,100 in the fiscal year 2009/10 to 256,422[130] in 2018. The number of crime scene profiles loaded onto the database has declined from 50,000 in 2008/09 to 37,487 in 2018[131].

136. In the fiscal year 2017/18, 130,520 subject profile records were deleted from the database[132] and 4,983 crime scene profile records were deleted.[133]

MATCH RATES

137. The extent to which crime scenes are examined for DNA stains varies significantly between offence types. 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. This is particularly so given cuts to policing resources during recent years. During my visits to police forces over the course of 2018 I have found that although most forces tell me that in theory they would attend and forensically examine any crime scene most have strict procedures in place to ensure that the crime scene investigation resources available are focused on serious incidents and those most likely to yield results.

138. Given that most of those convicted of a recordable offence will have their DNA and fingerprints retained,[134] 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 68.53% for England and Wales in 2018 which is fractionally higher than last year).

TABLE 10: Match Rate for Matches obtained immediately on loading for England and Wales Forces (year ending 31 December 2018)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	35,822	227,465
No. of Matches	24,550	4,551
Match Rate	68.53%	2.00%

Source: FINDS-DNA

128 This was in part due to deletions required by the newly enacted PoFA legislation.
129 This was the number of subject profiles held as of 31 December 2018. Previous reporting was for fiscal year. There were 6.20 million subject profiles held on the NDNAD at the end of fiscal year 2017/18.
130 This was the number of subject profiles added during 2018. Previous reporting was for fiscal year. There were 259,100 subject profiles added to the NDNAD during fiscal year 2017/18.
131 Previous reporting was for fiscal year. There were 40,100 crime scene profiles added to the NDNAD during fiscal year 2017/18.
132 Including automatic 'PoFA' deletions and deletions under the 'Deletion of Records from National Police Systems' Guidance; see also Chapter 6.
133 All these fiscal year figures are sourced from the FIND-SB Annual Report 2017/18 . Comparative figures are not available for calendar years due to ongoing issues with the management information that FINDS-DNA are able to obtain.
134 Whilst PoFA would allow all such biometrics to be retained, biometrics are not necessarily taken in all such cases.

TABLE 11: Match Rate for Matches obtained immediately on loading for all UK forces (year ending 31 December 2018)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	37,487	256,414
No. of Matches	24,989	4,991
Match Rate	66.61%	1.95%

Source: FINDS-DNA

ERROR RATES

139. Police forces and Forensic Service Providers (FSPs) have a number of safeguards in place to prevent and identify errors in processing DNA samples to gain a result that can be interpreted. Moreover, FINDS carry out daily integrity checks on the DNA profile records that are loaded onto the NDNAD. Error rates[135] that are found in the processing of DNA are generally acceptable (although it is noted that they are marginally higher than in 2016/17) for example sampling and record handling errors by FSPs are made in relation to just over 0.001% of subject profiles. Errors are made by FSPs when interpreting subject profiles in less than 0.003% of cases and in interpreting DNA profiles from crime-scenes in relation to around 0.2%.[136]

140. Since April 2016, data has been collected for FIND-SB on errors in DNA sampling by police forces, both at crime-scenes and in custody. This data is provided by the relevant police forces but last year I reported that seven forces had failed to provide the data. This year all forces provided at least some data on errors identified in force, although work is still being done to categorise the errors and ensure that reporting is uniform between forces. It is now possible to draw some early conclusions from the reported errors; for example, by the far the most common error during 2018 was failure to seal the bag containing the DNA sample. This highlights the importance of collating such data as this specific error could be attributed to a change in the manufacturing of the bags, which makes it more difficult to tell whether the bag has been sealed. These errors have now been reduced by ensuring that all relevant staff nationally are aware of the change and the need to double check the seal on the bag. It is reassuring to note that the majority of these errors are identified either by forces themselves before submission of the sample to the FSPs or by the FSPs when processing the sample. Nevertheless, integrity monitoring by FINDS does discover a small number of force handling errors on the NDNAD[137]. These errors occur in an average of around 0.07% of all subject profiles loaded to the NDNAD. While this is still very low it is almost double the rate of force handling errors discovered through integrity monitoring by the NDNAD during 2017.

141. Sample or record handling errors by police forces made when taking subjects' DNA samples have potential implications for the future detection of crime as where a sample cannot be submitted and/or profiled due to an error, and a replacement sample is not taken from the subject, the potentially important DNA data is lost.[138] On visits to police forces we have found that procedures for re-sampling vary but on the whole very few forces have defined processes

135 (i.e. the number of errors found through the DNA supply chain from sampling to matching against the NDNAD)
136 Figures are for fiscal year 2017/18, FIND-SB Annual Report 2017/18 p.29.
137 These occur when the DNA profile is associated with the wrong information.
138 At the very least additional police resources are needed to re-take the sample from the subject (who may well have left police custody).

for reporting failed samples and ensuring that the sample is re-taken. Some forces only re-take samples in relation to certain, more serious offences and others have no follow-up process at all beyond reporting the error to the officer in the case. It is therefore difficult to quantify the extent of DNA data losses arising from sampling or handling errors, even amongst forces who have reported their error rates to FINDS. Most of the 24 forces I have visited this year have received a recommendation that they implement a robust re-sampling procedure.

142. Errors on the NDNAD have the potential to affect NDNAD matching, i.e. the profile/record allows for missed matches, mismatch or elimination to occur. Were these errors not to be identified there is a chance, albeit a very small one, of a miscarriage of justice. Whilst it is important to acknowledge these risks, it is reassuring that police forces, regional scientific service hubs, FSPs and FINDS have such rigorous processes for checking and identifying errors in the DNA data that they receive.

NATIONAL FINGERPRINT DATABASE[139]

Additions to IDENT 1 in 2018[140]

143. IDENT1, as at 31 December 2018, held 8,203,873 unique arrestee subject tenprint records and 2,264,910 unmatched crime scene marks relating to 955,650 cases (see Table 8 above). During 2018, 818,565 unique subject records and 31,602 crime scene cases were created on IDENT1.

TABLE 12: Additions to IDENT1 (year ending 31 December 2018)

Tenprint sets from arrestees[141]	Individual subjects	Unmatched crime scene marks	Cases created with unidentified crime scene marks[142]
818,565	Data not available	145,847	31,602

Source: FINDS – National Fingerprint Office in consultation with IDENT1 supplier

TABLE 13: Deletions from IDENT1 (year ending 31 December 2018)

Tenprint sets from arrestees	Individual subjects	Unmatched crime scene marks	Cases with unidentified crime scene marks
132,396	49,729	146,653	Data not available

Source: FINDS – National Fingerprint Office in consultation with IDENT1 supplier

139 The statistical information available about the holding and use of fingerprints continues to be poor and not fit for purpose.
140 This data is for the main policing collections on IDENT1.
141 This is not comparable to the data shown in Table 10 of the 2017 report. It shows the total number of additions only, rather than the difference in database size, including additions and deletions.
142 Cases created may not be filed to the database.

144. During 2018, 49,729 PACE subject records[143] and 146,653 crime scene marks were deleted from the database. Deletions occur when retention rules mean that the record should no longer be maintained. The process to delete PACE subject records is largely automated as the PNC stores the retention rules and initiates deletion messages to IDENT1 accordingly.

MATCH RATES

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

TABLE 14: Fingerprint matches during 2018

	Scene of crime palm mark to palm print	Scene of crime fingermark to tenprint	Tenprint to scene of crime mark[144]
Total searches	90,324	478,709	Supplier data not correct
Number of matches	5,198	21,905	Supplier data not correct
Match rate	01:17.4	01:21.9	1:137.7

Source: FINDS – National Fingerprint Office in consultation with IDENT1 supplier

146. 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.[145]

KNOWLEDGE BASE ON USE OF BIOMETRIC EFFECTIVENESS

147. I have commented previously that a knowledge base on the effectiveness of the use of both DNA and fingerprints in police investigations does not exist, in part because it is very difficult to identify the added value from biometrics compared to other information available during

143 This data is from a different source to last year and differs significantly to the figure provided to me last year. This data has been provided in conjunction with the IDENT1 supplier.

144 Published match rate used as there is a discrepancy with the supplier data

145 DNA samples are usually taken in custody where a profile is not already held, in relation to major crimes or where an existing DNA profile has been obtained using SGM or SGM plus chemistries and the profile already held may require upgrading using the current DNA-17 profiling method. See further *National DNA Database Strategy Board Annual Report 2015/16* at paragraph 1.5.1.

an investigation.[146] The same point has been made by others and as part of the police's Transforming Forensics Programme[147] an attempt is now being made to quantify the benefits of biometrics used by the police but they have encountered similar problems.

148. Such an analysis will not be easy but it is necessary as the basis for future decision making about which biometrics should be deployed by the police. With the emergence of a range of new biometric technologies the need to understand the cost-effectiveness of different biometrics is becoming ever more important. In future the police will have a choice of a larger number of biometrics than presently. However, one would expect the marginal-value outcome to decline as the number of biometrics used increases. To guide their choices as to what is to optimal mix of the biometrics that are available the police will need to understand the relative utility and cost-effectiveness of each biometric. Cost data ought to be straightforward enough but quantifying effectiveness can be more difficult. The trials of the new biometric technologies have not yet tackled this work. A way needs to be found to design a *comparative* cost/effectiveness methodology which is as simple as possible but robust enough to guide the practical choices that will have to be made. The Home Office and the police might develop such a methodology together, so as to have a shared basis for their future decisions.

FOOTWEAR IMPRESSIONS

149. Footwear impressions are not a biometric but nevertheless they are included in PoFA. Section 15 of PoFA[148] 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."*[149]

150. Last year I reported that there is not an agreed national policy or even approach being applied to the retention of footwear impressions by all police forces in England and Wales. Indeed, not all forces routinely collect footwear impressions. The length of time for which footwear impressions are retained also varies and whilst some forces upload their impressions onto the national databases many do not.

151. There is no national data available on the use made of footwear impressions and the outcomes. FINDS announced that they are examining policy with regards to the retention and use of footwear impressions but so far no recommendations have emerged. In addition, a number of forces are re-examining their use of footwear impressions as part of their review of their budgets.

146 Commissioner for the Retention and Use of Biometric Material: *Annual Report 2016*, Section 2.4.
147 See: http://www.apccs.police.uk/police-reform/specialist-capabilities/
148 Which amends section 63F of PACE.
149 See: http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/1/enacted.

6. DELETION OF BIOMETRIC RECORDS

DNA SAMPLES

152. There are clear rules in PoFA as to when biometric samples should be destroyed.[150] Whilst PoFA allows the police to take DNA samples from all persons arrested for a recordable offence these must, as a general rule, be destroyed once a profile has been derived and certainly within six months. These rules were a central new element introduced by the PoFA legislation to reflect Parliament's decision that the information contained in a person's DNA sample was so sensitive that once the police had derived a DNA profile for criminal justice purposes the sample should be destroyed. However, other legislation allows the police to keep DNA samples until a criminal investigation and allied disclosure arrangements are concluded. This is an exception under the Criminal Procedure and Investigations Act 1996 (known as the CPIA exception)[151].

153. The majority of DNA samples taken under PACE were passed last year to one of three Forensic Science Providers (FSPs) for profiling and the FSPs have the responsibility for destroying 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. All the evidence that we have seen confirms that FSPs carry out destructions properly. The remaining PACE samples and the majority of DNA samples taken by the police for 'elimination' purposes are retained by individual police forces, either at their central forensic/scientific services hub or in property stores. Individual forces have responsibility for monitoring these samples and ensuring that they are destroyed in a timely manner. Since it is central to the regime introduced by PoFA that DNA samples should not be retained once a DNA profile has been derived I have monitored closely the destruction of DNA samples.

HAVE DNA SAMPLES BEEN APPROPRIATELY DESTROYED?

154. From the visits carried out to 24 police forces in England and Wales this year we have found no reason to suspect that, apart from the use of CPIA exception, which is discussed in more detail below, significant numbers of PACE DNA samples have been retained after profiles have been derived from them or for more than six months after the date they were taken.

CPIA EXEMPTION

155. As discussed earlier, whilst the general rule introduced by PoFA is that DNA samples should be deleted as soon as a DNA profile has been derived, an exception may be applied when a DNA sample is required for use in an ongoing investigation or if that DNA sample *"is, or may become, disclosable under the Criminal Procedure and Investigations Act 1996"*.[152] In such circumstances, the sample may be retained until it has fulfilled its intended use

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

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

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

(i.e. all of the required forensic analysis of the sample has been undertaken) or, if the evidence may be challenged in court, until the conclusion of judicial proceedings and any subsequent appeal proceedings.[153]

156. Since January 2016, all DNA samples that are held under the CPIA exemption beyond six months from the date they were taken, are required to be reviewed on a quarterly basis by the responsible police force. A record of that review process should therefore be available for audit purposes. Forces are also required to provided quarterly data returns to FINDS giving the number of both PACE and elimination samples they are retaining 'in force' under the CPIA exception. The FSPs also provide this information to FINDS for samples that they have been asked to retain, on a monthly basis.

157. DNA samples which are retained under the CPIA exception may be either:

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

158. Since January 2016, all elimination samples have been subject to the same retention rules as those taken from individuals arrested for recordable offences.[154]

159. It is possible for forces to take differing views as to the circumstances in which a DNA sample "*is, or may become, disclosable"* under the CPIA or any relevant code of practice – and it has been clear that forces in fact did so. This may be because there is an underlying problem with the CPIA exception. The wording of the exception, if taken literally to mean until all *possible* investigation and disclosure are completed, including, for example, a possible criminal cases review, could lead to all samples being retained because such possibilities are unpredictable. This would undermine the core PoFA principle of not retaining DNA samples beyond six months.

160. Last year I reported my concern that some forces were using the CPIA exception to routinely instruct FSPs to keep DNA samples whilst other forces were keeping much smaller numbers and deciding whether to do so on a case by case basis. I reported a rapid rise in the number of samples – both PACE arrestee and volunteer/elimination – held under this exception both 'in force' and with Forensic Service Providers. At least for some police forces in England and Wales, routine and/or 'blanket' retention of large numbers of DNA samples under CPIA had become their normal practice.

161. In my view the CPIA exception is just that, an 'exception' that allows the police to retain DNA samples for over six months in certain, very limited circumstances. If the CPIA exception were to be interpreted more widely, leading to the routine retention of samples by the police, then this would undermine the central element of PoFA on DNA sample retention. My predecessor therefore called for clearer guidance to be issued to the police on the use of the CPIA retention and Ministers agreed, in 2016, that *"further guidance on this issue would be beneficial"*[155]. It is disappointing to report that this guidance has still not been produced (see also Chapter 3).

153 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.
154 For further discussion of volunteer samples see: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016, 226-231.*
155 Ibid at paragraph 181.

162. In the absence of the Home Office issuing guidance on the use of this exceptional retention power and given the concerns just described, I wrote to all forces in December 2017 setting out my concerns and suggesting key principles in respect of the operation of the CPIA exception.[156] Since I regarded that letter as an interim measure until either the Home Office or FIND-SB provided forces with guidance, I regret to say that no guidance has in fact been given by either source.

163. We found on our visits to police forces this year that most of them had re-thought their use of the CPIA exception and overall there has been a reduction in the number of DNA samples being held beyond six months. However, a small number of forces are still holding DNA samples beyond the level that I regard as reasonable under the CPIA exception. A few forces are still applying a blanket retention policy for retaining DNA samples taken following certain types of offence, most commonly sexual offences. Their justification for this is that further analysis of the sample may be required. Whist it is certainly true that in some cases involving an allegation of a sexual offence further analysis of the DNA sample (most commonly Y-STR Analysis[157]) will be necessary this is not generally applicable to samples taken in relation to all sexual offence allegations. I have recommended to these forces that they urgently revise their policies.

164. Generally, in relation to samples taken under PACE, most forces that I visited were carefully monitoring all samples retained under the CPIA exception (usually with the FSPs) and were able to provide reasoning for each retained sample. This is a significant improvement on last year. Where I am still concerned is in relation to elimination DNA samples. These tend to be retained 'in force' unless they have already been submitted to the FSP for analysis and in most cases they are considered together with any other evidential material that has been gathered in the case. Where the elimination samples are retained at a central forensic/scientific hub they appear to be well monitored, with an auditable record kept of those samples retained under CPIA. Of concern, however, is the number of forces who are retaining these samples in their property stores, either a central property store or even local property stores. In the worst examples we have seen, forces were not able to say for certain how many elimination samples they were actually holding, particularly where these remained in local property stores. In quite a number of forces there was no robust procedure in place for monitoring elimination samples retained in property stores or deciding whether they still needed to be retained under the CPIA exception. This is unacceptable, particularly given the time that forces have now had to put such procedures in place, and I will continue to keep this under close review over the coming year.

165. 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 2018. These are set out below (Table 15). In relation to elimination samples, for the reasons given in the above paragraph the figures for samples retained in force may well be incorrect. In relation to those samples retained with the FSPs and PACE samples retained in force I have no reason to believe that these figures are not accurate. I reported last year that some forces had not provided the

156 A copy of this letter can be found in an Appendix D to last year's Report.

157 Y-STR profiling … is a highly sensitive forensic technique and, because it specifically targets male DNA, it is particularly useful for detecting and analysing a male suspect's DNA in a sample that contains a mixture of male and female cellular material. It is also a very useful technique for determining the number of men that have contributed to a mixed sample, as well as for linking male relatives. http://www.cellmarkforensics.co.uk/specialist_dna/ystrs.html

required data to FINDS for them to collate and report to my Office and others. Unfortunately, a number of forces are still not providing the required figures or are providing incomplete figures for their in force holdings to FINDS as requested, so the data is incomplete[158].

TABLE 15: DNA samples held under CPIA by England and Wales forces (31 December 2018)

	Total		Held in Force		Held by FSPs	
	2017	2018	2107	2018	2017	2018
Arrestee/PACE samples	7,952	6,952	1,184	1,190	6,768	5,762
Elimination samples	8,861	6,290	3,631	3,331	5,230	2,959

Source: FINDS-DNA

COPIES OF DNA PROFILES AND FINGERPRINTS

166. 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).

167. As regards copies of DNA profiles and fingerprints it remains the case that, apart from copy fingerprints that are being retained in the National Fingerprint Archive[159] or in case files, I have no reason to suspect significant non-compliance with section 63Q of PACE.

168. Some police forces do retain hard copy archives of fingerprints but none of the police forces visited during this reporting year maintains its own searchable database of fingerprints and each of them appears to have in place proper processes to ensure the identification of hard copy fingerprints which should no longer be retained.

169. I have, however, become aware this year of an issue which may affect the numbers of hard copy fingerprints that are being retained for an additional period going forward. In order to meet the requirements for ISO 17025 accreditation some fingerprint bureaux are choosing to print out marked up and annotated copies of fingerprint comparisons carried out by their fingerprint experts. I understand that this is because a detailed contemporaneous record must be kept of such comparisons, however printing this in hard copy is not necessarily required and is not the only way that this requirement can be met. These printed copies are then retained in case files[160]. I have been assured by forces undertaking this practice that copies are not searchable and are used only for the purposes of the case, nevertheless it does mean that more copies are now being printed, placed in case files and retained than was previously the case. Together with colleagues from the Forensic Science Regulator's Office I will be keeping this matter under close review.

158 Kent and Essex Police have not provided any figures for their end of year in force holdings and a number of forces, namely Gloucestershire, Bedfordshire, Gwent and South Wales were not able to provide figures for their in force holdings of elimination samples.

159 The Archive provides performance statistics on its operations to my Office on an annual basis. As is to be expected, the number of deletions of hardcopy fingerprint sets is reducing over time.

160 Case files are subject to review, retention and deletion rules as sent out in the College of Policing's Management of Police Information APP (MoPI).

DELETION OF POLICE RECORDS ORDERED BY CHIEF CONSTABLES

170. People whose biometrics are being lawfully retained by the police can apply for the 'early' deletion of their records from national police systems, namely the Police National Computer (PNC), the National DNA Database (NDNAD) and the National Fingerprint Database (IDENT1). This is referred to as the 'Record Deletion Process' (RDP). This process allows individuals to make an application for deletion of their PNC record and associated biometrics in respect of out of court disposals, NFA disposals and non-conviction disposals issued in court. Court convictions retentions are not eligible for review under the process. Making an application does not automatically mean that the individual's records will be deleted. Instead, the subject is provided with the opportunity to request that the force reviews the record(s) and makes a decision as to whether the information should be retained or deleted.

171. Although it is not a mandatory requirement for the application, individuals are encouraged to make out the ground(s) as to why they feel their record(s) should be deleted. This will support their request for deletion and enable the force to conduct a more thorough review compared to instances where a request for deletion is made with no reasoning provided. This depends, however, on a certain level of knowledge of the process and the ability of the individual to make out such a case.

172. The decision as to whether a record is retained or deleted from the aforementioned national systems is entirely at the discretion of the Chief Officer as Controller of the information (taking into account the national guidance[161] issued in respect of this process). Although this national guidance provides a steer for Chief Officers its application – the decision being discretionary – may vary from force to force. This is something that we have observed from talking to forces during visits and from a comparison of the proportion of deletions approved per force. It seems to me that whether a request for deletion will be approved remains somewhat a postcode lottery.

173. During the year ending 31 December 2018, 612 such deletions were approved by Chief Officers (see Table 16 below). Whilst these figures are not directly comparable to those in my previous Annual Report both the number of applications for deletion and the number of records approved for deletion have increased upon the previous year, although it must be noted that these deletions still represent only a very small proportion of those records that are potentially eligible for deletion. How far this constitutes a process that adequately provides for individuals to request that their biometrics be deleted is questionable with this level of take up.

161 An updated version of the guidance 'Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1) was published in January 2019. See the website of ACRO for details of making an application.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771892/Deletion_of_Records_from_National_Police_Systems__Guidance__v2.0.pdf

TABLE 16: Records Deletion Process (year ending 31 December 2018)

Total Applications received by ACRO Records Deletion Unit	Approved by Force	Rejected by Force	Rejected as ineligible by ACRO Records Deletion Unit	Pending with Force
1,865	612[162]	609	499[163]	140

Source: ACRO Criminal Records Office – Records Deletion Unit

162 Of these 17 were approved for partial deletion. In those instances the applicant is seeking the deletion of more than one arrest event/offence from their record but the force approves the removal of one (or two etc) but not all events/offences sought for deletion.

163 Of these 1,865, 1,361 were sent to forces. 499 were rejected due to ineligibility for the process and 5 await further information from the applicant (at the time of writing). Reasons for ineligibility include: no PNC record or record of event sought for deletion held on the PNC, court conviction sought for deletion, the applicant is the subject of a confirmed ongoing investigation or the applicant didn't respond to request for further information.

7. INTERNATIONAL EXCHANGES OF BIOMETRIC MATERIAL

174. One aspect of my role is that of overseeing the sharing of biometric material internationally. The Home Office's International DNA and Fingerprint Exchange Policy for the United Kingdom[164] 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."*

175. Many of the exchange mechanisms referred to in this chapter are EU mechanisms. Whether the UK will continue to have access to these mechanisms at the conclusion of the Brexit process is unknown until the Brexit process is completed. As I write, how Brexit will be completed is itself unknown.

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

177. In the absence of a policy for international fingerprint exchanges my advice, as it was of the previous Commissioner, to those involved was to mirror the processes in place for international DNA exchanges, but I urged that there should be revised guidance covering the international exchanges of both DNA and fingerprints.

178. FIND-SB has now produced this new guidance. A key issue in discussions about that new guidance was the extent to which international biometric exchanges should initially be anonymised, with the biographical detail associated with the biometric only shared if/when a match has been made. Previous guidance on the exchange of DNA profiles[165] followed this principle. However, law enforcement, particularly the National Crime Agency (NCA), have argued that the purpose for the international exchanges of DNA profiles and fingerprints is quite different. Their view is that DNA is primarily exchanged to see if a link between a crime scene stain and a known offender can be found and that initial exchanges can reasonably be anonymised until a link is established, whilst fingerprint exchanges are primarily used to confirm identity and therefore require biographical details to be attached at the time of exchange. I said last year that I was not convinced that this distinction can be easily made nor why it has the implication claimed. If fingerprint exchanges are to be treated differently than DNA then that would be a significant policy decision, which seems to me to be a decision for Ministers.

179. The new FIND-SB guidance has created the distinction suggested by the NCA between the international exchanges of DNA and fingerprints. I remain concerned that a body set up to oversee the DNA and fingerprint databases has made a policy decision that I think should be for Ministers. Given that most of the international exchanges at issue are EU exchanges then there seemed little point in pursuing this disagreement until the Brexit issue is settled.

---

164 Although this new policy has been approved by FIND-SB it is under further review and is therefore not published online. The previous policy which pertained to DNA only can be found at http://www.gov.uk/government/publications/international-dna-exchange-policy-for-the-united-kingdomhttp://www.gov.uk/government/publications/international-dna-exchange-policy-for-the-united-kingdom

165 DNA samples are very rarely exchanged.

Either these EU exchanges will be continued as part of a Brexit deal or, if we leave without a deal, they will cease. If we continue to be part of these EU exchanges then it is my view that Ministers should be asked to endorse FIND-SB's guidance, although the EU may set the terms of the exchanges in future in any event.

180. Law enforcement agencies are following this revised international exchange guidance but the guidance is not publicly available on the government website. This is because the guidance is being re-examined again in the light of the forthcoming Prüm exchanges (for which see below). It is difficult to regard this situation as satisfactory since one would normally expect that whatever international exchange policy was being followed was transparent and open to scrutiny.

THE ROLE OF UKICB, ACRO AND THE COUNTER-TERRORISM COMMAND

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

182. ACRO Criminal Records Office is a national police unit created originally by the Association of Chief Police Officers (ACPO) but now responsible to ACPOs successor the National Police Chiefs' Council (NPCC). ACRO oversees the international exchange of criminal records and the loading to the PNC of the foreign convictions of:

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

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

184. The Counter-Terrorism Command also exchanges biometric information, as well as intelligence, with foreign powers[166] and this is largely discussed in Chapter 4. During last year the Command brought to FIND-SB a proposal that they should be able to share DNA on the same basis on which they share fingerprints; so that for example they can share biometrically enabled watch lists with partner countries. This process allows the sharing of DNA data (taken in England and Wales) with selected countries with whom specific agreements have been made for sharing, in order to secure borders, and prevent and detect terrorist activity.

EXCHANGES OF FINGERPRINTS IN THE CONTEXT OF CONVICTION INFORMATION

185. ACRO exchanges criminal conviction data with the other 27 EU member states under Framework Decision 2009/315/JHA. Exchanges of the fingerprints of EU and UK nationals take place in response to 'Requests' or 'Notifications'.[167]

166 Particularly with EU partners.

167 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.

186. ACRO also exchanges conviction information and fingerprints with non-EU countries on behalf of the NCA and the Home Office. Those exchanges again take place in response to Requests and Notifications and may again involve the exchange of fingerprints.

187. Table 17 below provides comparative figures in relation to EU and non-EU exchange requests.

TABLE 17: Fingerprint Exchanges (year ending 31 December 2018)

	EU Exchanges	Non-EU Exchanges
Requests in	376	1,987
Requests out	12,872	5,864
Notifications in	3	22
Notifications out	3,514	6,677

Source: ACRO Criminal Records Office

EXCHANGE OF FINGERPRINTS AND DNA FOR INTELLIGENCE PURPOSES

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

DNA SAMPLES

189. DNA samples are only exchanged in very rare situations where the subject consents. On one occasion between 01 January 2018 and 31 December 2018 a DNA sample was exchanged. This was a kinship sample from a family member, sent from the UK to another European country in order to assist in identifying a deceased person whose remains had been discovered in that country.

DNA PROFILES

190. 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 and Fingerprint Exchange Policy for the United Kingdom* imposes strict limitations on the circumstances in which profiles may be exchanged. Table 18 below provides the figures for inbound and outbound DNA Requests.

191. There are 4 types of DNA profile enquiry that are dealt with by the NCA.[168]

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

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

193. *Inbound subject profiles*: DNA subject profiles are received from abroad and sent to FINDS-DNA for searching against the NDNAD. The Home Office Policy details the criteria under which searches will be authorised.

194. *Outbound crime scene profiles and profiles from unidentified bodies*: 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.

195. *Inbound crime scene profiles and profiles from unidentified bodies*: DNA crime scene profiles or unidentified body profiles may be received from abroad. The Home Office Policy states that, absent specific authorisation by FIND-SB, the UK will normally only comply with a request for the searching of an inbound crime scene profile if the relevant crime meets the definition of a 'UK Qualifying Offence'.[169] In every case consideration will be given to the question of whether or not "*the request and any subsequent search is necessary, reasonable and proportionate*".

TABLE 18: DNA Profile Enquiries (year ending 31 December 2018)

	Outbound from UK			Inbound to UK		
DNA Type	**Total**	**Searches concluded**	**Positive/ potential Match**	**Total**	**Searches concluded**	**Positive/ potential Match**
DNA samples	1	1	1	0	0	0
DNA subject profiles	23	7	0	125	118	15
Missing persons	9	3	0	68	64	3
DNA crime scene profiles	155	116	9	475	463	50
Unidentified bodies	13	13	1	104	91	11

Source: NCA

FINGERPRINTS AND FINGER-MARKS

196. There are 4 types of fingerprint enquiry dealt with by the NCA.

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

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

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

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

200. *Inbound crime scene finger-marks:* Foreign crime scene finger-marks 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.[170]

TABLE 19: Inbound and Outbound Fingerprint Requests (year ending 31 December 2018)

	Outbound from UK			Inbound to UK		
Fingerprint Type	Total	Searches concluded	Positive/ potential Match	Total	Searches concluded	Positive/ potential Match
Ten Print Sets	442	16	12	1,869	858	188
Crim Scene Fingermarks	33	0	0	160	6	2

Source: NCA

DIP SAMPLING

201. During a visit to the offices of the NCA in May 2018 my Head of Office and I dip-sampled cases where an international biometric exchange took place, some of which were exchanges of DNA and some of which were fingerprint exchanges. The DNA exchanges viewed were all in order and had been conducted according to Home Office policy. It was noted that where fingerprints were sent to other countries that these had the biographic details of the person from whom the fingerprints were taken attached. As noted above although this is in line with the newly issued (but not published) International Exchange Policy I have reservations about this approach.

202. I was made aware by the NCA in early 2018 that emails accompanying requests for international biometric exchanges had been sent which risked identifying the subject of an outbound DNA profile request. In these few cases, despite the specific request being anonymised, it was immediately followed by an email containing the fingerprints of the same person with biographic details attached. Actions have been taken to address the errors identified and also in order to prevent similar issues in the future.

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

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

EUROPEAN ARREST WARRANTS

204. The NCA is 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).

205. 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[171] and is responsible for recording all requests received through the Sirene system. All EAW requests, whether or not they have a UK connection, are now recorded, which has resulted in a higher number of recorded requests since 2014/15 than in previous years.

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

207. In the fiscal year 2017-18, 296 EAW requests were made by the UK and 17,256 EAW requests were received by it. Table 20 gives a yearly comparison since 2013[172]. During 2017/18 183 individuals were arrested and 181 individuals surrendered as a result of EAW requests made by the UK. In the same period 1,453 individuals were arrested and 1,027 individuals surrendered as a result of EAW requests made to the UK. It remains unclear whether or in what form the EAW system will continue after Brexit.

TABLE 20: EAW Requests by fiscal year (2013/14 – 2018/19)[173]

	2013/14	2014/15	2015/16	2016/17	2017/18
Requests from the UK	230	223	241	345	296
Requests into the UK	7,881	12,134	14,279	16,598	17,256

Source: NCA

LOADING NON UK CONVICTIONS ONTO PNC

208. 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,

171 '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).

172 All EAW requests, whether or not they have a UK connection, are now recorded, which has resulted in a higher number of recorded requests since 2014/15 than in previous years.

173 See https://nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/fugitives-and-international-crime/european-arrest-warrants?_highlight=WyJldXJvcGVhbiIsImV1cm9wZWFuJywiLCJldXJvcGVhbiculiwiYXJyZXN0liwiYXJyZXN0cyIsIm FycmVzd GluZyIsIm FycmVzdGVkliwid2FycmFudCIsIndhcn JhbnRzliwid2FycmFudGVkJyIsImV1cm9wZWFulGFycmVzdCIsImV1cm9w ZW FulGFycmVzdCB3YXJyYW50liwiYXJyZXN0IHdhcnJhbnQiXQ==

- 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.[174]

209. 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.[175]

210. In the 2015 Annual Report, my predecessor explained that that list, which has never been published, leaves scope for the exercise of judgement 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.

211. Although it was understood that relevant guidance would be finalised within weeks of that Report, no such document has been published. Nevertheless, when I visited ACRO in June 2018 I and my Head of Office had sight of the most up to date list and discussed with those operating the system the way in which the list is applied. There was nothing about those discussions which caused either of us any concern.

UK NATIONALS WHO HAVE OFFENDED ABROAD

212. 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.[176] 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.[177] 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.

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

175 The exceptions are convictions in countries with which the UK has appropriate bilateral Agreements i.e. Albania, Anguilla, Antigua, Barbados, Cayman Islands, Ghana, Jamaica, Montserrat, St Kitts and Nevis, St Helena and Ascension Islands, Trinidad and Tobago, Turks and Caicos, United Arab Emirates, United States of America, Sovereign Base Area of Cyprus.

176 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.

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

PRÜM

213. The Prüm Council Decisions of 2008[178] allow for the reciprocal searching of DNA and fingerprint databases within the EU on an anonymised 'hit/no hit' basis. The UK initially opted out of the Prüm exchanges. However, in December 2015[179] it was decided that the UK would rejoin the Prüm exchange mechanisms on the basis that proposed safeguards would be brought into force. Those safeguards were agreed by Parliament and include conditions to the effect:

- that only the DNA profiles and fingerprints of persons convicted of a crime will be made available for searching by other EU Member States;
- that demographic information about an individual will only be released following a DNA 'hit' if that hit is of a scientific standard equivalent to that required to report a hit to the police domestically in the UK;
- that such information will only be released in respect of a minor if a formal request for Mutual Legal Assistance has been made; and
- that the operation of the system will be overseen by an independent Prüm Oversight Board.

214. Both I and the Information Commissioner will have a role in overseeing and auditing Prüm exchanges.[180] What form that will take is not yet clear since the focus so far has been on gaining EU approval for the Prüm exchange to begin. I shall be concerned to ensure that, since the Prüm DNA exchanges will use an MPS Interface to facilitate those searches, proper governance arrangements are in place[181].

215. Following a successful DNA pilot scheme in 2015 the government has been working with EU partners to meet the technical and other conditions for joining Prüm. However, there have been numerous delays to the UK connecting to Prüm. Ongoing Brexit negotiations are likely to have contributed to these delays which also include delays by the European Parliament.

INTERNATIONAL EXCHANGES AND BREXIT

216. As I write the outcome of Brexit negotiations is unknown. Not all international exchanges depend on EU arrangements and regardless of the Brexit outcome, the UK will remain within broader exchange mechanisms such as Interpol. EU exchanges are presently the more numerous and straightforward of the exchanges being undertaken and the EU plans to make these even easier in the future by greater data sharing. Whether the UK is involved in the planning such future developments and whether we can make use of them will depend on the Brexit outcome.

217. Although the outcome of Brexit negotiations is unknown at the time of writing the government has made clear that it regards these biometric exchanges as important and that it considers it would be in the mutual interest to maintain the existing mechanisms. Furthermore, the government is shortly to join the EU Prüm Mechanism for the exchange of DNA, with fingerprint and vehicle number plate information exchange to follow.

178 2008/615/JHA and 2008/616/JHA
179 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.
180 See paragraph 7.7 of last year's Report.
181 HOB are building the capability for Prüm fingerprint exchanges within IDENT1.

218. If the Brexit outcome is that we lose access to EU exchanges and the EAW then that will be detrimental to the UK's ability to deal with inter-European criminal activity (including terrorism) and international crime with European links. The Home Office has given £2M to the police to put in place contingencies for such a loss and has set up a team under Assistant Commissioner Richard Martin of the MPS to plan for such an eventuality. However, the risks caused by losing EU exchanges and the EAW would remain for the future of policing.

8. APPLICATIONS TO THE COMMISSIONER TO RETAIN BIOMETRICS

219. 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'[182] but neither charged nor convicted.[183] In order for the police application to be approved they must persuade the Commissioner that retaining the biometrics will be useful in the detection, prevention or deterrence of crime.[184]

220. The person who is the subject of such an application must be notified by the police that an application has been made and must be told upon what grounds the application is being made. The subject of the application has the right to make their own representations to the Commissioner, challenging the application by the police for retention of their biometrics.[185]

221. 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. At the end of that period the police may apply to a District Judge for a further retention period of two years. The relevant statutory provisions are set out in full at Appendix B.

APPLICATIONS

222. From when the relevant sections of PoFA came into force on 31 October 2013 to 31 December 2018, 570 such applications to the Commissioner were received. Of those applications:

- 1 application was submitted in 2013
- 126 applications were submitted in 2014
- 123 applications were submitted in 2015
- 136 applications were submitted in 2016
- 108 applications were submitted in 2017
- 76 applications were submitted in 2018[186]

223. In the last year, the number of cases submitted to my office has decreased to between 6 and 7 per month. In 2016, the number of forces submitting cases to my office peaked at 19 forces. In 2018 this figure reduced to 15 forces.

224. The great bulk of the 250 applications submitted up to 31 December 2015 were made by the Metropolitan Police Service (MPS) and during that period only 9 of the other 43 forces in England and Wales made applications. Since January 2016 a far larger number of forces have submitted applications and that figure has now risen to 29. 14 forces have yet to make an application – see further Table 21. During 2018 the MPS made 14 of the 76 applications to the Commissioner, with the other 62 made by 14 different forces.

182 Generally more serious violent, sexual offences, terrorist offences burglary and robbery. See: The Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013.
183 Under section 63G of PACE as inserted by PoFA.
184 Under section 63G(4) of PACE.
185 See section 63G(5) and (6) of PACE and further https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace The Commissioner will require that the arrestee be informed 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.
186 Different time periods have been used from previous annual reports, to better reflect the number of cases received by the OBC per calendar year.

225. The reduction in the number of applications made by the MPS this year to only 14 is of particular note given their previous relatively prolific use of this process. As recently as 2017 they made 50 applications and the MPS has a dedicated Biometric Retention Unit which I am given to understand still has three members of staff. It would appear that the reduction in the number of applications may be related to the problems the MPS are experiencing with updating PNC at the end of an investigation, so by the time Unit receives cases to consider they are already outside the 28 day application period (see also Chapter 3 paragraphs 68-71).

Table 21: Number of Applications to the Commissioner by Force (year ending 31 December 2018)

Force	2018	Total Applications since 31 Oct 2013
Metropolitan Police	14	354
Yorkshire and Humberside[187]	15	55
Kent	8	26
Northumbria	6	19
Thames Valley	7	18
Devon and Cornwall	6	15
Cambridgeshire	2	13
South Wales	0	13
Dorset	7	8
Essex	2	7
Bedfordshire	0	6
Hertfordshire	0	6
West Mercia	0	6
North Wales	2	4
Warwickshire	0	4
Avon and Somerset	3	3
Greater Manchester	0	3
Cleveland	1	2
Cumbria	0	1
Derbyshire	0	1
Durham	0	1
Gloucestershire	0	1
Gwent	1	1
Lincolnshire	1	1
Norfolk	0	1
Wiltshire	1	1
TOTAL	**76**	**570**

187 Collaboration on biometric retention consisteing of Humberside, North Yorkshire, South Yorkshire and West Yorkshire.

226. In the five years since the introduction of the PoFA Regime on 31 October 2013 (i.e. to 31 December 2018), applications to the Commissioner were received and determined as follows.

Table 22: Applications to the Commissioner to Retain Biometrics for Qualifying Offences Under s63G PACE

	31 October 2013 to 31 December 2017	1 January 2018 to 31 December 2018
Total Applications	**494**	**76**
– Representations from subjects	61 (12.3%)	8 (10.5%)
Concluded by end of 2018[188]	**494**	**70**
Approved	317 (64%)	48
Rejected	118 (24%)	17
Withdrawn	59 (12%)	5

LEGAL BASIS FOR APPLICATIONS TO THE COMMISSIONER

227. 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).

228. Between 31 October 2013 and 31 December 2018, 314 applications were made in relation to victim characteristics and 256 were made for the more general purpose of the prevention or detection of crime.[189] In a number of the former, more than one of the 'victim criteria' were satisfied.

Table 23: Statutory Basis for Applications to the Commissioner (31 October 2013 – 31 December 2018)

	Applications received[190]	Approved	Refused[191]
Victim criteria[192]			
– under 18	262	156	104
– 'vulnerable'	25	16	9
– associated with subject of application	27	11	15
Prevention/detection of crime	256	185	71

188 Cases concluded during 2018 do not correlate exactly with cases received in 2018 as there is necessarily a time lag between receiving and concluding a case.

189 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.

190 Including cases invalid or withdrawn;

191 Some cases are yet to be determined.

192 In some cases more than one of the victim criteria are satisfied. Figures in the table relate only to the primary victim criterion give.

PRELIMINARY APPLICATIONS

229. 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.

230. In fact, matters of disclosure have arisen only relatively rarely and to 31 December 2018 only 15 such applications have been made. All bar one of these preliminary applications have gone on to become full applications.

APPLICATIONS TO A DISTRICT JUDGE

231. Whilst I can consent to the retention of biometrics for those arrested for, but not charged with, a qualifying offence, that retention period will only be for a maximum of three years from the date the biometrics were taken. The retention period for those charged with, but not convicted of, a qualifying offence is similarly three years. If the police wish to retain the relevant biometrics for a further period of two years in either circumstance they can apply to a District Judge.[193]

232. My last Annual Report recorded that by 31 December 2016 6 applications to a District Judge had been made. As far as I am aware no further applications have been made.

THE APPLICATIONS PROCESS

233. Applications are made to the Office of the Biometrics Commissioner (OBC) electronically by the police. The police are required to provide me with details of the case about which the application is being made and to give reasons as to why they believe retention is appropriate. The police must also provide supporting documentation such as crime reports, CPS decisions and a printout from the PNC. A notification letter, detailing the application and reasons for it should also be sent by the police to the subject of the application.

234. In every instance, the subject of an application is told if that application has been refused or approved. Where an application is approved, detailed reasons are only provided as a matter of course to subjects who have made representations to me.[194] 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. 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.

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

193 See Section 63F of PACE as inserted by section 3 of PoFA.

194 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.

ON WHAT GROUNDS DOES THE COMMISSIONER DECIDE APPLICATIONS?

236. In order to make an application the police have to demonstrate that, whilst the subject was not charged for the offence at issue, there is evidence to show that it is likely that the subject of the application was involved in the act, that retaining the biometrics for three years will either be a deterrent to future criminal action or aid in the prevention or detection of future crime, and finally that the interference in the subject's privacy is proportionate given the public benefit that is likely to result. I must weigh the evidence on each of these factors, in each case, before reaching a decision. The Commissioner's core principles and approach to assessing these relevant factors is set out in a guidance document issued by FINDS-SB called *Applications to the Biometrics Commissioner under PACE*.[195]

237. 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;[196] or
- charging the subject would not be in the public interest.[197]

238. If the former, the subject of an application may regard it as strange that where there is insufficient evidence to justify charging them with the offence there can be sufficient grounds to justify retention of their biometrics. In fact the so-called 'charging threshold' used by the CPS to decide whether to charge requires that the evidence is such for there to be a realistic prospect of conviction and that depends on judging how far the evidence is likely to stand up to cross examination. However, I am not bound to consider the evidence against the subject to the higher criminal standard, instead I will require that the criteria as set out in the guidance document are satisfied and that retention of the subject's biometrics is considered 'appropriate'.

239. It is noteworthy that although the number of representations to me by the subjects of applications is small, in those I have received the subject often objects to an application on the grounds that the police have investigated their actions but it has been decided not to proceed with a prosecution, so in their eyes that demonstrates they are innocent. The legal complexities are such that the decision not to proceed with a prosecution does not necessarily demonstrate innocence, but the confusion is understandable. If, for example, 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.

195 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/764558/Applications_to_the_Biometrics_Commissioner_under_PACE__September_2018.pdf (see also Appendix B).

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

197 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.

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

241. Even if both these conditions are fulfilled, I must judge whether retaining the biometrics would be proportionate in the particular case by balancing the public benefit from retention against the interference in individual freedom that it will involve. Where the subject is under the age of 18 I must additionally bear in mind the principle established in *S and Marper v United Kingdom*[198] that *'particular attention should be paid to the protection of juveniles from any detriment that may result from the retention … of their private data'*,

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

WHAT TYPE OF OFFENCES LEAD TO APPLICATIONS?

243. Only 'qualifying offences' can be the basis of an application but, as can be seen in Table 24, the majority (61%) of applications are for sexual offences.

Table 24: Outcome of Applications to the Commissioner to Retain Biometrics for Qualifying Offences under section 63G PACE (31 October 2013 – 31 December 2018)

Offence Group	Total applications	Approved	Refused	Withdrawn
Murder, Attempts and Threats to Kill	13	6 (46%)	6 (46%)	1 (8%)
Sexual Crimes	345	203 (59%)	106 (31%)	33 (10%)
Assaults	92	64 (70%)	11 (12%)	16 (18%)
Robbery	64	53 (83%)	2 (3%)	9 (14%)
Burglary	42	30 (71%)	11 (26%)	1 (3%)
Other	14	11 (79%)	1 (7%)	2 (14%)
Total[199]	570	367	137	62

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

198 (2008) 48 EHRR 1169 at paragraph 124
199 4 cases from 2018 are still to be decided.

245. A particular feature of the applications received by my Office in the last two years has been the increase in applications related to sexual contact between young people. The CPS has extensive guidelines in respect of charging for sexual offences. One is to the effect that the charging decision for sexual offences should be the same as for other offences but with a more proactive approach to evidence building.[200] Conversely, the guidelines also advise that it may not be in the public interest to criminalise sexual behaviour, especially between young people[201], and therefore balancing these guidelines can be difficult. For example, sexual penetration between a 14 year old male and a 12 year old female is rape, even if both parties say they freely consented, and so such an offence should be charged. On the other hand, the offence involves sexual behaviour between young people and a decision may be taken that prosecution of those involved would not be in the public interest. If the latter decision is made the police may, and often do, choose to apply to retain the biometrics of those arrested.

246. 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. Sometimes such cases also involve a subject who themselves is vulnerable whose needs also need to be considered. In such scenarios, it remains open to the police to apply to retain the biometrics of those accused.

247. 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.

248. It is evident from the applications received by my Office that there is a general belief amongst the police that minor sexual offending, or familial sexual offending, will lead to sexual offending of increasing gravity or stranger attacks. There is some evidence to support this belief but it is by no means conclusive[202] and in any case the evidence refers to overall statistics and does not provide a basis for predicting the future behaviour of an individual.

249. 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.

250. Last year we started to collect such evidence by examining the outcomes in terms of re-offending for those who had been the subject of a section 63 application. The analysis in last year's report was heavily caveated because it was still too early to draw any conclusions, given the limited length of time that had passed and the size and limitations of the data set. This year that analysis has been repeated and extended by Jessica Mullins of ACRO[203] to whom I am very grateful. Even now there are still some of the same limitations but if this can

200 See: http://www.cps.gov.uk/legal/p_to_r/rape_and_sexual_offences/cps_policy_statement/

201 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 alleged abuse or exploitation.

202 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

203 I am grateful to Rob Price the CEO of ACRO for seconding Jessica to my office for a period in order to carry out this analysis. A report of the analysis can be found at Appendix D.

be repeated each year it will build into a knowledge base against which the police can decide which possible cases are most worth pursuing and should help the Commissioner make more informed judgements.

251. The analysis focused on all applications made to the Commissioner since PoFA came into force and decided upon prior to 16th November 2017[204]. The focus of the analysis was largely on the applications in which a decision was made to either approve or refuse the extended retention of the biometrics, discounting those that had been withdrawn or rejected. The dataset was therefore of 387 cases.

252. This year the analysis suggests:

(i) 74% of the 387 applications were approved by the Commissioner. Therefore, in three quarters of cases examined and decided upon, the Commissioner was in agreement that it was appropriate in all the circumstances to retain the subject's biometrics.

(ii) Of the 288 approval decisions made, 118 individuals came to police notice again following the arrest which resulted in the application. This equates to 41% of all subjects of approved applications. To some extent one might therefore conclude that in almost half of cases the approval of the application has been demonstrated to be appropriate. What is almost impossible to measure, however, is deterrent effect. It is therefore not possible to say how many, if any, of the 59% of subjects who did not come to notice again would have done so had it not been for the retention of their biometrics.

(iii) Of these 118 individuals who came to notice again half came to notice for a similar alleged offence or the same alleged offence and the other half came to notice for an alleged offence different in nature to that which was subject of the application.

(iv) It was not unusual for those who came to notice again to do so on multiple occasions, indicating that some of these individuals have become persistent offenders. This includes 69 subjects who had two or more subsequent arrests and particularly the 13 individuals who were arrested on 10 or more subsequent occasions.

(v) In relation to the 99 refusal decisions made, 27 individuals came to police notice again; 27% of all refusals. This equates to 7% of the total number of decisions made by the Commissioner. It could possibly be concluded that in these 7% of cases, given that the subject has come to police notice again, there may have been benefit to retaining their biometrics. It is difficult to say this with any certainly as it would depend on the specific circumstances and nature of the new police contact. It is also not possible to ascertain whether fewer subjects would have come to notice again as a result of the deterrent effect of their biometrics being retained, had the application been approved.

(vi) Of the 387 applications, 126 were made in relation to subjects who were under the age of 18 at the time of the alleged offence. Of this 126, 66 subjects (52%) came to police notice again. Therefore, although there were fewer applications made in respect of minors, those which were made were made in relation to subjects who were more likely than adult subjects to come to police notice again.

204 These were all decisions over a year old at the time the data was gathered.

(vii) 238 applications out of the total 387 (61%) related to sex offences. In 171 of these cases the subjects were 18 years or over at the time of their arrest and 67 individuals were under the age of 18 at the time of their arrest.

(viii) For adults, of the 171 initially arrested for a sexual offence 35 came to police notice again, 18 of which were for a further sexual offence. Therefore in 11% of cases where the subject of the application was arrested for a sexual offence the subject came to notice again for a sexual offence. The situation is similar for minors where of the 67 individuals initially arrested for a sexual offence 25 came to police notice again, nine of which were for a further sexual offence. Therefore in 13% of cases where the subject of the application was arrested for a sexual offence the subject came to notice again for a sexual offence. This is a relatively small proportion and appears to support the view that only a small proportion of those arrested for a sexual offence will go onto commit a further sexual offence.

253. In addition to the above analysis DNA barcodes were submitted to the National DNA Database (NDNAD) to ascertain whether the retained DNA profile had ever resulted in a match against a crime scene mark and from what offence that crime scene mark originated. These barcodes related to 119 DNA profiles belonging to individuals who had been the subject of an approved s.63G application[205]. The data returned indicated that 24 matches were identified against crime scene marks held within the NDNAD in respect of 17 subjects. This means that in relation to just over 4% of approved applications we know that the retained DNA profile was of definite use in making a match. Given that in less than half of approved cases is the profile still being retained (and could therefore be checked for matches) it might be possible to extrapolate and approximate that in 9% of approved cases the retained DNA profile was of use in a further investigation. This analysis is limited and would need to be extended in future years to reach more concrete conclusions in relation to the usefulness of retained profiles (and fingerprints were this analysis also to be done).

WHY DO SO FEW SUBJECTS OF APPLICATIONS CHALLENGE THE POLICE CASE TO THE COMMISSIONER?

254. Parliament was careful in legislating to allow the subject of an application to the Biometrics Commissioner to challenge that application by making representations but to date only a small minority of the subjects have done so – see Table 25.

Table 25: Representations by Subjects and Outcomes (31 October 2013 – 31 December 2018)

Applications	Totals	Representations made by the Subject of the Application
Approved Applications	365	38 (10%)
Refused Applications	135	27 (20%)

205 In some instances a DNA profile was previously retained but the PNC record confirmed that the material had been destroyed (due to the expiry of the three year period), there was therefore no DNA barcode recorded on the record because the profile had been deleted from the database.

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[206]. More worrying is if subjects believe that they will not be listened to or that they simply wish, following an NFA for an alleged offence, to bring to an end what has been a lengthy and stressful experience. The low rate for the submission of representations is a problem in that it suggests that the protection for subjects of an application intended by Parliament is not working as expected.

255. In autumn 2018 we began an experiment in which we are offering to some subjects an option simply of phoning my Office if they wish to challenge the police application and explaining why. It is too early yet to say whether that has increased the number of subjects raising a challenge/making representations but I will report on this in my next report.

REPRESENTATIONS FROM CHILDREN AND YOUNG PEOPLE

256. I also remain concerned about the low numbers of representations received from children and young people, given the general policy necessarily adopted by my Office and the police to address correspondence only to the subject of an application (including children and young people[207]) unless and until they expressly authorise us to do otherwise, due to concerns about privacy and sensitivity of personal information. In my view 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. As detailed in Chapter 3 (paragraphs 74 to 75) efforts have been made to tackle this problem but at the time of writing a satisfactory solution has still not been implemented.

BIOMETRICS COMMISSIONER 'UZ' MARKERS

257. 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. This marker remains until the application is decided, at which point it must be removed if the application is refused. If the application is approved the marker remains in place for three years from the date the biometrics were taken. 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. This enables me to monitor the number of UZ markers in use and to check the data provided against my own records of applications made to me.

258. As of December 2018, a total of 242 UZ markers were in use by forces in England and Wales. That figure breaks down as follows:

206 In general the offender population has relatively high levels of poor literacy and education compared to the general population as well as higher rates of mental illness and drug taking: see, e.g.: http://www.prisonerseducation.org.uk/media-press/new-government-data-on-english-and-maths-skills-of-prisoners and publications.parliament.uk/pa/cm201213/cmselect/cmhaff/184/18409.htm

207 *Commissioner for the Retention and Use of Biometric Material, Annual Report 2017*, paragraphs 151-156.

TABLE 26: Biometrics Commissioner 'UZ' Markers by Force (December 2018)

Metropolitan Police Service	72
Northumbria Police	11
Noth Yorkshire Police	1
West Yorkshire Police	22
South Yorkshire Police	1
Humberside Police	4
Cleveland Police	1
West Mercia Police	2
Warwickshire Police	2
Cambridgeshire Constabulary	2
Bedfordshire Police	13
Essex Police	2
Thames Valley Police	13
Kent Police	21
City Of London Police	23
Devon & Cornwall Police	9
Gloucestershire Constabulary	1
Dorset Police	7
North Wales Police	4
Gwent Police	1
South Wales Police	30
Total	**242**

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

- There have continued to be instances of the inappropriate use of a UZ marker, for example where a UZ marker has simply been erroneously applied or applied and then no formal application for retention under section 63G PACE has been made. If such a marker remains incorrectly the biometrics may be retained unlawfully. My Office review the markers on a monthly basis and will continue to keep this under close review over the coming year.
- There have been a number of instances where a force have made an application to me but have failed to apply a UZ marker to the PNC. In the absence of the such a marker the biometrics have been automatically deleted 14 days after the NFA date and force have had no choice but to withdraw the application.

260. 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 have largely been resolved by the changes to the bail process set out in the Policing and Crime Act 2017. The only remaining markers of this type are being used by City of London Police in relation to fraud cases dating back to before 2017[208].

208 I require City of London Police to provide me with regular updates on these investigations and to justify the continued use of the marker in this way. They have not always been timely with these updates and without such a justification the markers will need to be removed.

APPENDIX A

THE 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[209]

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.

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.

209 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.'

In this context a 'recordable offence' is, broadly speaking, any offence which is punishable with imprisonment[210] 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.[211]

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 1 at paragraph 12 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.[212]

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.

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.[213]

- 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'.

210 See section 118 of PACE
211 See (new) section 65B of PACE and section 65 of the Crime and Disorder Act 1998.
212 See section 65A(2) of PACE
213 See section 63K of PACE (as inserted by section 7 of PoFA)

– 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

10. 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

11. 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.[214] In such cases biometric material may be held on the basis of an NSD for a 2-year period. NSDs may be renewed before the date of their expiry for as many times as is deemed necessary and proportionate (see further **Appendix C**).

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

12. 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[215], the resulting 3 year retention period may be extended for a further 2 years if, following an application by the relevant Chief Officer under section 63F(7), a District Judge so orders. The decision of the District Judge may be appealed to the Crown Court.

CONVICTIONS OUTSIDE ENGLAND AND WALES

13. By section 70 of the Crime and Policing Act 2017, which amends sections 63F, 63H, 63I, 63J, 63K and 63N of PACE, Police may retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample of persons convicted of a recordable offence under the law of a country or territory outside England and Wales where that offence is equivalent to a recordable offence in England and Wales. It should be noted that UK convictions under the laws of Scotland and Northern Ireland are treated as 'foreign convictions' for the purposes of biometric retention. This will only apply to biometrics taken in England and Wales on or after 03 April 2017[216].

14. For those persons whose biometrics were taken by police before 03 April 2017, by sections 61(6D), 62(2A) and 63(3E) of PACE[217] the police have, with the authority of an officer of the rank of inspector or above, power to take fingerprints and a DNA sample from any person who has been convicted outside England and Wales of an offence that would constitute a qualifying offence under the law of England and Wales. By section 63J of PACE[218] the police have the power to retain for an indefinite period any such fingerprints and any DNA profile derived from such a sample. Although section 63J allows the police to retain for an indefinite period biometric material which has been taken under sections 61(6D), 62(2A) or 63(3E), it has no application to biometric material that has been or is taken under any other

214 See sections 63M and 63U of PACE as inserted by sections 9 and 17 of PoFA) and Schedule 1 of PoFA.
215 (as inserted by section 3 of PoFA)
216 Although the relevant provisions were commenced on 03 April 2017 the Home Office have not yet completed the work needed for these changes to be brought fully into effect on the PNC or issued the necessary guidance.
217 (all inserted by section 3 Crime and Security Act 2010)
218 (inserted by section 6 PoFA)

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

APPENDIX B

APPLICATIONS TO THE BIOMETRICS COMMISSIONER UNDER SECTION 63G PACE

The Relevant Statutory Provisions

1. Section 63G of PACE provides as follows.

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

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

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

(ii) On the face of things, a chief officer may make an application under section 63G(2) provided only that they consider that an alleged victim of the alleged offence was, at the time of that offence, under 18, *"vulnerable"* or *"associated with"* the arrestee.[219] 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*

219 These terms are defined at section 63G(10).

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[220], no indication is given as to the extent (if any) to which that person must be told of the reasons for the application or of the information upon which it is based.

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

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

4. In practice, an application to retain biometric material under section 63G PACE must usually be made within 28 days of the date on which the relevant individual is NFA'd[221]. [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.]

STRATEGY BOARD GUIDANCE AND CORE PRINCIPLES

5. 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.[222] The Strategy Board endorsed the approach which the Commissioner had decided to adopt as regards such applications and the detailed

220 Further relevant provisions are at sections 63G(7) to (9).

221 There have been some difficulties with this approach during 2018, as some forces have failed to update PNC with the NFA outcome at the end of an investigation. The approach relies on PNC being updated in a timely manner at the end of an investigation, otherwise by the time the NFA entry is made it is already more than 28 days after the conclusion of the investigation. See also Chapter 3 paragraphs 68-71.

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

Guidance document which it issued in September 2013 (and into which my predecessor had significant input) was consistent with a document issued by my Office around that time entitled *Principles for Assessing Applications for Biometric Retention.*

6. During 2018 my Office carried out a review of all our casework practices and documents. As part of that review it was decided that the Guidance document and *Principles* document were so similar that it would be simpler for police forces to have one single guidance document to refer to. A new, revised, Guidance document was therefore proposed and was issued by what is now the FINDS Strategy Board in September 2018. A copy of the Strategy Board Guidance can be found at https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace

7. The key provisions of the Guidance are as follows.

    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 of the reasons for any application and of the information upon which it is based. The reasons must be sufficiently detailed, so that the subject has a fair opportunity to make representations to the Biometrics Commissioner. 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:*

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

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

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

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

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

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

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

OBC DOCUMENTS

8. 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.

APPLICATIONS TO DISTRICT JUDGES (MAGISTRATES' COURT)

9. If the Biometrics Commissioner accedes to an application under section 63G(2) or (3), by section 63F of PACE[223], 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.[224]

223 (as inserted by section 3 of PoFA)
224 See further Appendix A: Applications to District Judges (Magistrates Court)

APPENDIX C

NATIONAL SECURITY PROVISIONS

Statutory Background and Guidance as to NSDs

Statutory Background

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

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

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

3. PoFA introduced stricter rules as regards the retention by police forces anywhere in the United Kingdom of biometric material which has been obtained from unconvicted individuals pursuant to TACT, the CTA or the TPIMs Act. The police and other law enforcement authorities may retain DNA profiles and fingerprints for an extended period on national security grounds but they may only do so pursuant to a National Security Determination or 'NSD'.[225]

4. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[226] 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,[227] in practice the same 2-year maximum is applied. An NSD may be renewed before its expiry for a further period of 2 years.[228]

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.

---

225 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.

226 (i.e. the Chief Officer or Chief Constable of the force or authority that 'owns' the biometric records at issue). The NSD determination may be made by any Chief Officer once the biometric provisions of the Counter-Terrorism and Border Security Act 2019 (CTBS Act) come into force.

227 (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)

228 The period of 2 years will be extended to 5 years once the biometric provisions of the CTBS Act come into force.

6. NSDs may be made or renewed under[229]:

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

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

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

   - every person who makes or renews an NSD must within 28 days send to the Commissioner a copy of the determination and the reasons for making or renewing it;
   - every such person must also disclose or provide to the Commissioner such documents and information as the Commissioner may require for the purposes of carrying out the review functions which are referred to above; and
   - if on reviewing an NSD the Commissioner concludes that it is not necessary for any material retained pursuant to the determination to be so retained, the 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[231] as issued can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf.

229 NSDs will also be able to be made under paragraph 46 of Schedule 3 to the CTBS Act once it comes into force.
230 (see footnote 225 above).
231 New Statutory Guidance must be issued before the once the biometric provisions of the CTBS Act can come into force.

NSD PROCESS

Applications for NSDs

12. Applications for NSDs are compiled and submitted to Chief Officers by the MPS Counter-Terrorism Command 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."* [232]

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:

> *"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.

232 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."*

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.

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 the MPS/PSNI.

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

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

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.[233]

233 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.

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.

(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[234] the police and relevant law enforcement agencies were given two years (i.e. until 31 October 2015) to assess that material and to decide whether or not to apply for NSDs in relation to it. Parliament further agreed in October 2015 a one year extension of that transitional period until 31 October 2016[235]. 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 2016, 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:

234 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)

235 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)

Provision	Relevant Material	Retention Period[236]
Paragraph 20B Terrorism Act 2000 (TACT)	DNA profiles/fingerprints relating to persons detained under s.41 TACT.	3 years[237]
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.

236 The retention period starts from the date the relevant DNA sample/fingerprints were taken unless otherwise stated.
237 Once the biometric provisions of the CTBS Act come into force DNA profiles/fingerprints relating to persons arrested for terrorism offences under PACE will also be subject to a 3 year retention period.

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 the MPS's Secure Operations Forensic Services (SOFIS). The CT Fingerprint Database is a separate and secure database within IDENT1 for CT-related fingerprints and crime scene fingermarks. It is also operated solely by SOFS.

27. In January 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.

APPENDIX D

Home Office

Department for Digital, Culture Media & Sport

Data Protection Act 2018

Factsheet – Law enforcement processing

(Sections 29 – 81)

What does the Act do?

- Updates our data protection laws governing the processing of personal data for law enforcement purposes by the police, prosecutors and others.
- Strengthens the rights of data subjects, whilst ensuring that criminal justice agencies and others can continue to use and share personal data to prevent and investigate crime, bring offenders to justice and keep communities safe.
- Ensures that, following the UK's exit from the European Union, our criminal justice agencies can continue to share data with partner agencies in other EU Member States and remain at the forefront of the international effort to tackle serious organised crime and other threats to our security.

City of London Police Commissioner Ian Dyson QPM, National Police Chiefs' Council lead on information management, said:

"The new Data Protection Act replaces its 20th century predecessor with modern legislation and a package of reforms that protect both individuals and organisations, strengthens the regulator and introduces a bespoke framework for law enforcement.

"It is vital that policing is enables us to perform our duties by maintaining public approval of our actions. In a digital age the way we handle personal data; how we collect, store, use and dispose of it is coming under growing scrutiny. In return for willing cooperation, the public expect a proportionate balance across law enforcement of how we manage their information."

Home Office | Department for Digital, Culture Media & Sport

How does the Act do it?

The Act provides a bespoke framework for law enforcement processing, tailored to the needs of the police, prosecutors and others (referred to in the Act as "competent authorities"). This framework will protect the rights of victims, witnesses and suspects while ensuring we can continue to effectively tackle crime and other threats to community safety, both at home and abroad.

Background

Since the advent of the Data Protection Act 1998, advancements in technology have led to increasing rates of personal data processing and transferral, both internally and cross-border. An increase in the collection and sharing of personal data comes with the need for a stronger and more coherent framework for the protection of personal data.

In April 2016, the EU agreed the Law Enforcement Directive (LED) to govern "the processing of personal data by the police and other criminal justice agencies for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data". The LED applies in relation to the cross-border processing of personal data for law enforcement purposes. To ensure a coherent regime, the provisions in Part 3 of the Act also apply to the domestic processing of personal data for such purposes. This ensures that there is a single domestic and trans-national regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.

Home Office | Department for Digital, Culture Media & Sport

Key law enforcement data processing provisions

Part 3 of the Act strengthens the rights of data subjects whilst enabling a controller to restrict these rights where this is necessary to, amongst other things, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences, for example by revealing to a person that they are under investigation. This Part:

- Sets out six data protection principles which apply to law enforcement processing by a competent authority. The requirements are that:
  - ➔ processing be lawful and fair;
  - ➔ the purposes of processing be specified, explicit and legitimate;
  - ➔ personal data be adequate, relevant and not excessive;
  - ➔ personal data be accurate and kept up to date;
  - ➔ personal data be kept no longer than is necessary; and
  - ➔ personal data be processed in a secure manner.

- Sets out the rights of individuals over their data. These include:
  - ➔ rights of access by the data subject to information about the data processing (including the legal basis for processing, the type of data held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint);
  - ➔ the right to rectification of inaccurate data and of erasure of data (or the restriction of its processing) where the processing of the data would infringe the data protection principles; and
  - ➔ rights in relation to automated decision-making (that is, decision making that has not involved human intervention).

- Places restrictions on those rights, but only where necessary and proportionate in order to:
  - ➔ avoid obstructing an investigation or enquiry;
  - ➔ avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
  - ➔ protect public security;
  - ➔ protect national security; and
  - ➔ protect the rights and freedoms of others.

Home Office
23 May 2018

APPENDIX E

ACRO Criminal Records Office

Office of the Biometrics Commissioner

Review of the applications made under Section 63G of the Police and Criminal Evidence Act 1984

February 2019
Jessica Mullins

1 Background

1.1 The introduction of Section 63G[1](s.63G) of the Police and Criminal Evidence Act 1984 (PACE), as amended by the Protection of Freedoms Act 2012 (PoFA), introduced provisions which enables police forces to make applications to the Biometrics Commissioner to request the extended retention of fingerprints and DNA (biometrics) in specific circumstances where the provisions of PoFA do not extend to automatic retention.

1.2 This applies only for individuals who have been arrested and given a 'No Further Action' (NFA) by the police in respect of a Qualifying Offence[2] and where there are no existing mechanisms on the PNC record which allow for the continued retention of the biometrics *and* whereby the force has a concern about that individual.

1.3 In such instances, the force can make an application to the Office of the Biometrics Commissioner (OBC) requesting a 3-year retention commencing from the date that the samples were obtained.

1.4 During the application process, and to prevent the deletion of the biometrics once the NFA disposal has been added to the PNC record, the force must add a Wanted/Missing marker using reserved force station code 'UZ'. If the Biometrics Commissioner approves the application, then the wording of the marker must be updated by the force to reflect that the retention of the biometrics has been authorised.

1.5 If the application is refused, then the force must remove the marker as soon as possible to allow for the automatic weed of the biometrics thus preventing any unlawful retention of this material.

2 Research Project – s.63G applications

2.1 On the 8th November 2018, I joined the OBC for a period of 3 months to carry out some research in respect of the s.63G applications made to the Biometrics Commissioner by police forces in England and Wales.

2.2 The main purpose of this research was to analyse the applications that have been submitted to the OBC over a set period of time to determine whether those individuals have come to police notice since, for what sorts of alleged offences and to see if there are any patterns. The effect upon the biometric retention periods in respect of any subsequent arrest events will also be analysed in this report.

2.3 In reviewing this information, it will perhaps provide an indication as to whether being the subject of an application, whether approved or rejected, acts as a deterrent to commit further crime or not.

2.4 This report will also compare the data of individuals who were under the age of 18 (U18) at the time of the arrest which resulted in the s.63G application against those that were 18 or over (O18) at the time of their arrest.

2.5 A further area of focus will also look at sex offences for the simple fact that they make up a large proportion of the s.63G applications that the OBC receives.

[1] https://www.legislation.gov.uk/ukpga/1984/60/section/63G
[2] As defined in 65A(2) of the Police and Criminal Evidence Act 1984

2.6 A small piece of comparative analysis has also been conducted relating to under 18's in respect of the two top offences where retention is applied for under the s.63G process to determine whether there was any potential 'missed opportunities' for making applications for extended retention.

2.7 Finally, a short piece of work was completed in respect of DNA profiles taken and still held against an arrest which resulted in a s.63G application which were run through the National DNA Database (NDNAD) to determine whether there were any hits against crime scene marks.

3 Overview

3.1 From the commencement of PoFA on the 31st October 2013 to the 8th November 2018[3], the OBC received a total of **554** applications from forces.

3.2 Not all forces in England and Wales have utilised the application process which is reflected in the fact that during this period, **21 forces** have made valid s.63G applications which represents less than half. However, it should be noted that the s.63G application procedure is not a process which forces *must* engage with – it is simply available as mechanism to potentially enable extended biometric retention for those individuals which are deemed to be a concern.

3.3 I will also add that, during this same period, a further two new forces did submit a s.63G application however, both were subsequently withdrawn by the respective force.

3.4 See Annex A for a breakdown of the volumes of applications submitted by forces which were subject of this research.

3.5 Of the 554 applications that were made between 31st October 2013 and November 8th 2018, **461** requests were valid and progressed to the conclusion of a decision to approve or retain during this same period.

3.6 Applications were deemed to be invalid or withdrawn for several reasons:

3.6.1 Withdrawn due to the biometrics already being held indefinitely.

3.6.2 Withdrawn as a marker was not added to the record to hold the biometrics and so they automatically weeded.

3.6.3 Application was submitted after the 28-day timeframe.

4 The criteria applied to the research

4.1 **Criteria 1** – Of the 461 applications, a decision was made to focus on those applications which were at least a year old or more. Therefore, only applications which were decided upon prior to 16th November 2017[4] were reviewed. This was because a sufficient amount of time needed to have passed from when the initial arrest was carried out in order to provide some meaningful data.

[3] 31st October 2013 represents the commencement of the s.63G process and the 8th November 2018 marks the commencement date of my secondment.

[4] 16th November 2017 marks the date of the last decision made during that month.

4.2 **Criteria 2** – Of these applications, the focus was largely on the applications which were taken through to a conclusion to either authorise or refuse the extended retention of the biometrics. However, a small piece of analysis has also been conducted towards the end of this report in respect of the applications which were withdrawn.

4.3 This results in an initial data set of **387** applications which forms the basis of the statistical analysis that underpins this report[5]. Please note that this figure only applies to applications which were **approved or rejected**.

4.4 The data was broken down by year within which the decision was made (2014-2017). Although the s.63G process commenced in tandem with PoFA on the 31st October 2013, the first valid s.63G application wasn't received by the OBC until 20th January 2014.

4.5 The data was elicited from two sources. Firstly, the master record where the OBC logs the applications that they receive from forces and secondly, the Police National Computer (PNC) as the PNC is the national database where forces record events which confirms whether an individual has been arrested, charged, summonsed, reported or subject of a postal requisition.

4.6 The PNC is also where the police / courts / law enforcement agencies record the disposal in respect of an event. The disposal then determines the retention period applied to the fingerprints and DNA through specific scripts introduced to the PNC once PoFA came in to being.

4.7 This analysis did not extend to the local systems held within police forces and where certain incidents / intelligence is also recorded. Only those events which are recorded on the PNC, through the aforementioned reasons stated in 4.5, will have an effect upon the retention of fingerprints and DNA.

4.8 For the purposes of data protection, all data referred to this in report has been completely anonymised.

5 Overview

5.1 The following table provides a breakdown in respect of the 387 applications decided upon between 01/01/2014 and 16/11/2017.

Year of decision	Approve retention	Refuse retention	Approval %	Refusal %
2013	0	0	0%	0%
2014	39	7	85%	15%
2015	68	17	80%	20%
2016	118	58	66%	34%
2017	63	17	79%	21%
TOTAL	288	99		

[5] The remaining 93 applications (of the 554 applications referred to at 3.5) were either withdrawn by the force (60), rejected by the OBC as invalid (3) or were outstanding (30) awaiting review at the point of writing.

5.2 This clearly indicates that the Biometrics Commissioner makes more decisions to approve the extended retention of biometrics in respect of the applications that his office receives – the figures represent an approval rate of 74% in respect of the applications reviewed as part of this data set.

5.3 Although not hugely remarkable, 377 of the applications made were in respect of males, and just 10 were in respect of females who were aged 18 years or over and therefore classed as adults.

5.4 7 of the 10 applications made in respect of a female were for an alleged offence against the person and 3 of the female subjects came to police notice on a subsequent occasion – only one resulted in a conviction leading to the indefinite retention of the biometrics. Please see table below.

Date of original arrest	Age at time of arrest	Decision	Alleged offence subject of s.63G application	Arrest since s.63G application	Alleged Offence	Biometric status
01/01/2014	35	Approved	Attempted Murder (Victim 1 Year Or Over)	Y	Destroy or Damage Property (£5000 Or Less)	Weeded
14/12/2013	32	Approved	AOABH	N	N/A	Weeded
26/06/2014	27	Rejected	Aggravated Burglary (Comprising Commission of an Offence in Dwelling)	N	N/A	Weeded
07/05/2014	31	Approved	Causing Grievous Bodily Harm W/I To Do GBH	Y	Battery	Weeded
26/07/2014	18	Approved	Robbery	Y	Possess Controlled Drug - Class B - Cannabis/Resin Possessing Controlled Drug W/I To Supply - Class B - Other Possess W/I To Supply Controlled Drug - Class B - Cannabis Possessing Controlled Drug - Class B - Cannabis Possess Controlled Drug - Class B - Cannabis/Resin	Indefinite
28/02/2015	21	Approved	Kidnap/False Imprison A Person W/I To Commit A Relevant Sexual Offence	N	N/A	Weeded
21/08/2106	55	Rejected	Manslaughter	N	N/A	Weeded
22/08/2016	24	Rejected	Manslaughter	N	N/A	Weeded
29/10/2016	18	Approved	Wounding W/I To Do GBH	N	N/A	Held due to UZ marker
29/10/2016	18	Approved	Wounding W/I To Do GBH	N	N/A	Held due to UZ marker

5.5 All of the 387 applications were subject to a check on the PNC as this source would confirm whether or not the individual had come to police notice since their last arrest which, resulted in the force making the s.63G application.

5.6 The following was concluded in respect of the initial review:

5.6.1 From 01/01/2014 – 16/11/2017 a total of **288 applications** were approved.

5.6.2 From 01/01/2014 – 16/11/2017 a total of **99 applications** were rejected.

5.6.3 Out of the 387 applications, **242 subjects have not come to police notice** since the arrest which resulted in the s.63G application. 170 of these were approved s.63G applications and the remaining 72 were rejected.

5.6.4 This is further confirmed by the fact that the biometric status for the 242 who have not come to police notice since the arrest which resulted in the s.63G application is either:

1) Not held as they've fallen to automatic destruction (177 subjects) or;

2) Held due to a live Wanted/Missing UZ marker (65 subjects)

5.6.5 Table 4 of Annex B contains a further breakdown in respect of the 242 subjects who have not come to police notice again.

5.6.6 However, **145 subjects did come to police notice** between the period of the arrest which resulted in the s.63G application and the point at which the PNC check was conducted[6]. This will be discussed in more detail in section 6.

6 Subsequent police notice

6.1 A full overview in respect of subjects who came to subsequent police notice can be found at Annex B. Tables 1, 2 and 3 show a breakdown in terms of the arrest volumes, U18 / O18 and the current biometric status.

6.2 The 145 subjects who came to subsequent police notice represents a percentage of 37% of the total subjects (387) decided upon between 01/01/2014 and 16/11/2017 (no decisions were made in 2013).

6.3 Of the 145 subjects, the outcome of their s.63G application breaks down as follows:

Year of decision	Arrest since s.63G	Approvals	Rejections
2014	26	21	4
2015	38	34	5
2016	56	41	15
2017	25	22	3
TOTALS	145	118	27

6.4 81% of subjects who came to notice had been the subject of an approved s.63G application and 19% of subjects who came to notice had been the subject of a rejected s.63G application.

6.5 The subsequent police notice of these 145 subjects did have a varied effect upon the biometric status.

6.6 In respect of the individuals who saw **no change** to the status of their biometrics at the time that the check was conducted due to their subsequent police notice (56 subjects), the fingerprints and DNA were either still being held due to a live UZ marker (13 subjects) or they had fallen to automatic destruction (43 subjects) because the UZ marker had expired or they had come to police notice for a further event or events which resulted in 'No Further Action'.

Biometric status change due to subsequent police notice?	2014	2015	2016	2017	TOTALS
Yes	18	25	30	16	89
No	8	13	26	9	56
					145

[6] PNC checks conducted between 08/11/2018 – 29/11/2018

6.7 In respect of the remaining 89 subjects who did see a change in the retention status of their biometrics due to the new arrest(s), 68 had come to notice and were given a disposal which resulted in the indefinite retention of their biometrics, please see table below for a further breakdown.

Indefinite retention	2014	2015	2016	2017	TOTALS
Court Conviction	12	13	17	9	51
Caution	3	6	0	1	10
Conditional Caution	1	0	2	1	4
Youth Caution	0	0	2	0	2
Youth Conditional Caution	0	0	1	0	1
					68

6.8 The remaining 21 subjects saw a temporary amendment to the status of their biometrics as a result of the new event that they came to notice for.

Temporary retention	2014	2015	2016	2017	TOTALS
Ongoing investigation	2	6	3	5	16
2 years - Penalty Notice for Disorder	0	0	2	0	2
3 years – Arrested/charged not convicted of a Qualifying Offence	0	0	1	0	1
WM Entry	0	0	2	0	2
					21

6.9 In terms of the offence categories for which the 145 individuals came to notice, these were widely varied with the top 4 offence categories being drugs offences, theft and kindred offences, offences against the person and sex offences.

Offence category[7]	2014	2015	2016	2017	TOTALS
1 - Offence Against the Person	4	8	8	4	24
2 - Sex Offences	1	7	12	2	22
3 - Offences Against the Property	2	0	1	2	5
4 - Fraud and Kindred Offences	0	1	0	0	1
5 - Theft and Kindred Offences	6	4	10	5	25
6 - Offences Against The State	0	0	0	0	0
7 - Public Disorder and Rioting	3	0	2	1	6
8 - Offences Relating to Police/Courts/Prison	3	0	4	0	7
9 - Drugs	2	12	8	7	29
10 - Offences Related to Immigration	0	1	0	0	1
11 - Firearms/Shotguns/Offensive Weapons	5	3	1	2	11
12 - Miscellaneous	0	2	10	2	14
TOTAL	26	38	56	25	145

6.10 Although not particularly remarkable, there was a small minority of just 13% of the 145 subjects whereby the subsequent alleged offending resulted in a term of imprisonment.

[7] Offences recorded on the PNC are categorised between 1-12 depending upon the 'type' of alleged offence.

Imprisonment since s.63G	2014	2015	2016	2017
Yes	3	8	5	3
No	23	30	51	22

7 Arrests and Approvals

7.1 Whilst section 6 provides a general overview of figures in respect of the whole data set for those who came to police notice again following the arrest which resulted in the s.63G application (387 subjects), I will now further breakdown this analysis by discussing those whose biometrics were **approved** for extended retention by the Biometrics Commissioner and who have since come to police notice.

7.2 288 applications submitted to the Biometrics Commissioner and decided upon between 01/01/2014 – 16/11/2017 were approved and thus resulted in the 3-year retention of the subject's fingerprints and DNA.

7.3 Of these approvals, **118 subjects** have come to police since the arrest which resulted in the s.63G application. This represents a percentage of 41% which is neither high nor low but perhaps indicates that being subject of an approved s.63G application does not, particularly, act as a deterrent to commit further alleged offences.

7.4 In respect of individuals who came to notice on **more** than one occasion (58%) following the s.63G application, the nature of the alleged offending differed widely as indicated at 6.9.

7.5 Alleged offences were also reviewed to determine whether the individual came to notice for again for a similar or the same alleged offence to that subject of the s.63G application. The data concluded an exact 50% split with 59 individuals coming to notice for **a similar alleged offence or the same alleged offence** and the other 59 individuals coming to police notice for an alleged offence different in nature to that which was subject of the s.63G application.

7.6 The nature of subsequent police notice differed widely, as alluded to above, in part because it was not uncommon that subjects came to notice again on more than one occasion and for more than one alleged offence – out of the 118, 69 subjects had 2 or more arrests following the arrest relative to the s.63G application.

1 arrest	49	49
2 arrests	22	69
3 arrests	12	
4 arrests	7	
5 arrests	4	
6 arrests	1	
7 arrests	3	
8 arrests	4	
9 arrests	3	
10 arrests	6	
12 arrests	2	
14 arrests	1	
15 arrests	1	
16 arrests	2	
21 arrests	1	
		118

7.7 Furthermore, whilst looking at the 118 data set as whole, there was a large number of drugs offences that were present with 48 of the 118 individuals coming to police notice for such an alleged offence. Currently, no drugs offences feature on the Qualifying Offences list but there are plans in the future by the Home Office to address this.

7.8 80 of the 118 subjects had also subsequently come to notice for a Qualifying Offence or for more than one Qualifying Offence, the disposals of which were varied. However, data was also captured specifically in respect of the first arrest event following the s.63G application which impacted upon the retention of the biometrics or not. Analysis concluded that 16 of the 80 subjects came to notice for a Qualifying Offence which saw a change in the retention of their biometrics.

7.9 In respect of biometric retention, further analysis was done and concluded that of the 118 subjects, 73 had an amendment to the retention of their fingerprints and DNA.

7.9.1 57 subjects of those 73 now have indefinite retention applied to their fingerprints and DNA as they have since been convicted in court or given a caution.

7.9.2 13 individuals are currently subject to ongoing investigation by the police and so, their fingerprints and DNA are being retained due to the presence of an ongoing investigation marker.

7.9.3 2 individuals have had a further 2 years applied to the retention of their fingerprints and DNA as they were issued with a Penalty Notice for Disorder.

7.9.4 1 individual had a further 3 years applied to the retention of their fingerprints and DNA as they were arrested, charged but not convicted of a Qualifying Offence.

7.9.5 10 of those individuals of those 57 who now have indefinite retention applied to their biometrics were arrested in respect of a Qualifying Offence.

7.10 Of the 73 subjects, the arrest data breaks down as follows in terms of how many times the individual has been arrested since the arrest resulting in the s.63G application and how that subsequent arrest or arrests impacted on the retention of their biometrics.

Arrest volumes post s.63G	Totals	Indefinite retention	Ongoing investigation	2-year retention[8]	3-year retention[9]
Arrests 1-5	50	37	10	2	1
Arrests 6-9	11	9	2	0	0
Arrests 10+	12	11	1	0	0

7.11 What can perhaps be deduced from the above is that the decision made in respect of the s.63G application was often proportionate and due to the overlap in respect of the subsequent arrest meant that the biometrics held in respect of the s.63G arrest could continue to be retained as opposed to the police taking new samples (unless there was an upgrade required in respect of the DNA).

[8] 2 year retention applied in respect of a Penalty for Disorder

[9] 3 year applied in respect of being arrested, charged but not convicted of a Qualifying Offence

7.12 In order to test this assumption, all 73 records were reviewed in terms of the new event date which created a new retention period against the date of the arrest which resulted in the s.63G application to determine whether the biometrics approved for a 3 year retention continued to be kept as a result of a subsequent event.

7.13 In the majority of cases, the sample date of the biometrics tends to be the same date (give or take a day) that the individual is arrested.

7.14 61 of the 73 subjects came to notice within the 3 years and so, this meant that any biometrics taken / held in respect of the s.63G application could continue to be lawfully retained.

7.15 51 of the 61 subjects either received a court conviction or a caution / conditional caution / youth caution which resulted in the indefinite retention of the biometric material.

7.16 Therefore, the remaining 10 had a retention period which was either limited to 2 or 3 years because they had received a Penalty Notice for Disorder (2 subjects) or because they had been arrested, charged but not convicted of a Qualifying Offence (3 subjects). Or, it was yet to be determined because the biometrics were being held due to an ongoing investigation marker (5 subjects).

7.17 The final 12 subjects who came to police notice for an event which affected the retention period of their biometrics were either convicted at court, given a caution or are currently subject to an ongoing investigation however, this occurred outside the 3-year retention period applied following the approved s.63G application.

7.18 Annex C provides a breakdown of this data accordingly.

7.19 Under 18's are discussed in further detail later on in this report. However, in respect of the data set of approved applications and subsequent police notice, 47 of the 118 subjects were under 18 at the time of the arrest which resulted in the s.63G application.

7.20 28 of the 47 subjects now have indefinite retention applied to their biometrics. Furthermore, the alleged offences for which they came to subsequent notice, and I say 'offences' because all of the 47 individuals were arrested on 2 or more occasions, did not appear to follow any particular pattern.

7.21 Although drugs, theft, assault and possession of a weapon/knife offences appeared frequently throughout the 47 data set which is unsurprising as, although not quantified, many records in this data set indicated gang related activity.

7.22 Headline Figures:

- 41% of individuals whose biometrics were approved for retention under the s.63G process came to police notice again.
- 62% of individuals whose biometrics were approved for retention under the s.63G process and came to notice again, came to notice for an event which saw a further amendment to the retention period of their biometrics.
- 78% of individuals whose biometrics were approved for retention under the s.63G process and came to notice again, came to notice for an event which resulted in the indefinite retention of their biometrics.
- 40% of individuals' subject of an approved application and who came to notice again were under the age of 18 at the time of the arrest resulting in the s.63G application.

- 68% of individuals whose s.63G application was approved and came to notice again, came to notice in respect of a Qualifying Offence.

8 Arrests and Refusals

8.1 Similar to section 7, this part of the report focuses solely on those applications which were refused under the s.63G process and the individuals who subsequently came to police notice again.

8.2 99 applications submitted under s.63G were refused by the Biometrics Commissioner between 01/01/2014 – 16/11/2017. Of these subjects, just over a quarter (27% which represents 27 individuals) have come to police notice since their arrest.

8.3 In respect of individuals who came to notice on **more** than one occasion following the s.63G application, which totalled 14 subjects, the nature of the alleged offending again, differed widely.

8.4 As with the approvals, the 27 records were also reviewed to determine whether the individual came to notice for again for a similar offence to that subject of the s.63G application. The data concluded that 48% (13 subjects) came to notice for **a similar alleged offence or the same alleged offence** and with the remaining 14 individuals coming to police notice for an alleged offence different in nature to that which was subject of the s.63G application.

8.5 Of those 13 who came to notice for a similar or the same alleged offence, 2 individuals were convicted of the offence in court and one individual was given a caution therefore, this resulted in the indefinite retention of their fingerprints and DNA.

8.6 At the time of writing, a further 2 individuals were actively being investigated by the police and so the ongoing investigation marker recorded on the PNC is retaining the fingerprints and DNA until a conclusion is reached.

8.7 Please see Annex D for a complete breakdown of these findings.

8.8 As the table below indicates, 52% of the 27 subjects came to notice on two or more occasions.

1 arrest	13	13
2 arrests	4	14
3 arrests	3	
4 arrests	2	
6 arrests	1	
8 arrests	1	
11 arrests	1	
12 arrests	1	
15 arrests	1	
		27

8.9 17 of the 27 subjects had also subsequently come to notice for a Qualifying Offence or Qualifying offences with varied disposals. Again, data was also captured specifically in respect of the first arrest event following the s.63G application which impacted upon the retention of the biometrics or not. Analysis concluded that 5 of the 17 subjects came to notice for a Qualifying Offence which saw a change in the retention of their biometrics.

8.10 Of the complete data set of 27, 15 individuals saw an amendment to the retention of their fingerprints and DNA.

8.10.1 11 subjects of those 15 now have indefinite retention applied to their fingerprints and DNA as they have since been convicted in court or given a caution for a further offence.

8.10.2 3 individuals are currently subject to ongoing investigation by the police and so, their fingerprints and DNA are being retained due to the presence of an ongoing investigation marker.

8.10.3 1 individual has a Wanted/Missing (WM) Locate Trace marker currently keeping the biometrics.

Arrest volumes post s.63G	Totals	Indefinite retention	Ongoing investigation	WM entry
Arrests 1-5	10	6	3	1
Arrests 6-9	2	2	0	0
Arrests 10+	3	3	0	0

8.11 In respect of under 18's, a large proportion of the rejected applications where subjects came to police notice again following the s.63G application were within this data set - 70%, which represents 19 subjects. 11 of these individuals went on to be arrested on 2 or more occasions, and as before, the alleged offences for which they came to notice were varied in nature with drugs, theft and possession of a weapon/knife making a regular appearance in the event histories.

8.12 Headline Figures:

- 27% of individuals whose biometrics were rejected for retention under the s.63G process came to police notice again.
- 56% of individuals whose biometrics were rejected for retention under the s.63G process and came to notice again, came to notice for an event which saw an amendment to the retention period of their biometrics.
- 73% of individuals whose biometrics were rejected for retention under the s.63G process and came to notice again, came to notice for an event which resulted in the indefinite retention of their biometrics.
- 70% of individuals' subject of a rejected application and who came to notice again were under the age of 18 at the time of the arrest resulting in the s.63G application.
- 63% of individuals whose s.63G application was rejected and came to notice again, came to notice in respect of a Qualifying Offence.

9 Subjects 18 Years or Over – General Overview

9.1 Of the 387 s.63G applications made to the OBC, 261 applications were in respect of individuals who were 18 years or over at the time of their arrest. 201 applications were approved and 60 applications were refused.

9.2 A total of 79 subjects [10] aged 18 or over at the time of the s.63G application have come to notice again.

[10] Out of a total of 145 subjects referred to at 5.6.6.

9.3 Of the refusals, just 8 individuals came to police notice again and this breakdown is outlined in the table below.

Year of decision	Age at time of arrest	Total arrests on record	Offence category subject of s.63G application	Number of arrests since s.63G	Alteration to biometric due to new arrest(s)?	Category of new alleged offence	Offence code	Qualifying offence?	Disposal type	Current biometric status?
2014	85	9	2	8	Y	7	7.6.17.1	Y	Conviction	Indefinite
2014	41	6	2	3	Y	8	8.7.65.1	N	Caution	Indefinite
2015	22	2	2	1	N	10	10.1.2	N	No Further Action	Weeded
2015	24	3	2	1	N	2	2.1.4.2	Y	No Further Action	Weeded
2016	31	2	2	1	N	2	2.8.19.1	Y	No Further Action	Weeded
2016	20	2	2	1	N	2	2.1.4.2	Y	No Further Action	Weeded
2016	44	3	2	1	Y	2	2.8.16.1	Y	Conviction	Indefinite
2017	18	7	5	3	Y	12	12.2.138	N	Caution	Indefinite

Note: In respect of 'category of new alleged offence'- this refers to the alleged offence which then amended the biometric retention on that record OR in the event of no further action and there was no effect upon the biometrics other than weeding, it refers to the alleged offence for which they next came to notice for following the arrest which resulted in the s.63G application.

9.4 Of the approvals, 71 individuals out of 201 came to police notice again. The effects upon the biometric retention of their subsequent arrest(s) is as follows:

Indefinite retention: 30
Held due to an ongoing investigation: 7
Held for 2 years due to a Penalty Notice for Disorder: 2
Held due to a Wanted/Missing marker under UZ: 5
Biometrics now weeded: 27

Note: 2 of the subjects whose biometrics are held due to a Wanted/Missing marker also have an ongoing investigation marker on file. However, until the outcome of that investigation is determined, the Wanted/Missing marker trumps the ongoing investigation marker in terms of biometric retention.

9.5 Of the 261, 2 subjects have been arrested on 10 or more occasions since the s.63G application was made. One subject continued to come to notice for a series of alleged offences against the person such as Battery, Wounding/Inflicting GBH and Common Assault. They were also subject to further arrests for the same alleged offence which resulted in their s.63G application; Assault Occasioning Actual Bodily Harm.

9.6 The second subject whose s.63G application was made in respect of a sexual assault did not come to notice for any further sexual offences. The nature of their subsequent alleged offending was varied in nature and including numerous driving offences, Robbery, Kidnapping and Affray.

9.7 Both subjects had applications approved for the extended retention of their fingerprints and DNA however, they have since been convicted and so the retention of their biometrics is now indefinite.

9.8 The other 5 subjects came to notice on a further 6-9 occasions. What's interesting about the 7 aforementioned subjects is that aside from one, despite being 18 or over, they are in their 20s and are still relatively young.

Year of decision	Outcome	Age at time of arrest	s.63G alleged offence	Similar or same alleged offence to s.63G?	Number of arrests	Change	New status
2014	Rejected	85	Exposure	Y	8	Y	Indefinite
2014	Approved	23	AOABH	Y	10	Y	Indefinite
2014	Approved	20	Causing Grievous Bodily Harm W/I To Do GBH	N	7	Y	Indefinite
2015	Approved	19	Sexual Assault - Intentionally Touch Female - No Penetration	Y	10	Y	Indefinite
2016	Approved	27	Burglary and Theft - Dwelling	Y	9	Y	Indefinite
2016	Approved	18	Burglary and Theft - Dwelling	Y	8	Y	Indefinite
2016	Approved	18	Robbery	Y	7	Y	Indefinite

10 Under 18 Subjects – General Overview

10.1 126 subjects were under the age of 18 at the time of their arrest. 87 applications were approved and 39 applications were refused.

10.2 A total of 66 subjects of the above figures have come to notice again, many of whom will now be aged 18 years or over.

10.3 Of the refusals, 19 individuals came to police notice again and this breakdown is outlined in the table below. This represents 49% of the U18's whose s.63G application was rejected.

Year of decision	Age at time of arrest	Total arrests on record	Offence category subject of s.63G application	Number of arrests since s.63G	Alteration to biometric due to new arrest(s)?	Category of new alleged offence	Offence code	Qualifing offence?	Disposal type	Current biometric status?
2014	16	8	1	6	Y	11	11.6.4.1	N	Conviction	Indefinite
2014	15	23	5	15	Y	11	11.6.37	N	Conviction	Indefinite
2015	14	13	2	12	Y	9	9.1.5.23	N	Conviction	Indefinite
2015	15	6	5	1	N	1	1.8.12	Y	No Further Action	Weeded
2015	16	4	2	2	Y	1	1.8.11.2	N	Caution	Indefinite
2016	13	2	2	1	Y	12	12.15.12	N	Conviction	Indefinite
2016	10	4	2	2	Y	5	5.6.1.1	N	No Further Action	WM Entry
2016	14	2	2	1	N	9	9.1.5.23	N	No Further Action	Weeded
2016	13	5	2	4	N	5	5.5.6.1	N	No Further Action	Weeded
2016	12	3	1	2	N	7	7.1.7.1	N	No Further Action	Weeded
2016	15	14	5	11	Y	5	5.3.7	Y	Youth Caution	Indefinite
2016	12	5	2	4	Y	9	9.1.5.23	N	Youth Conditional Caution	Indefinite
2016	13	2	2	1	N	12	12.6.7	Y	No Further Action	Weeded
2016	15	3	2	2	N	9	9.1.5.23	N	Not Guilty	Weeded
2016	13	2	2	1	Y	2	2.1.4.2	Y	Impending Prosecution	Impending
2016	15	2	1	1	N	9	9.1.5.23	N	No Further Action	Weeded
2016	12	2	12	1	Y	2	2.8.16.1	Y	Impending Prosecution	Impending
2017	12	4	2	3	Y	5	5.8.2.2	N	Impending Prosecution	Impending
2017	16	3	12	1	N	12	12.2.138	N	No Further Action	Weeded

10.4 Of the approvals, 47 U18 individuals out of the 87 came to police notice again. The effects upon the biometric retention of their subsequent arrest(s) is as follows:

Indefinite retention: 28
Held due to an ongoing investigation: 6
Held for 3 years as arrested charged but not convicted of a qualifying offence: 1
Held due to a Wanted/Missing marker under UZ: 7
Held due to a different Wanted/Missing marker: 1
Biometrics now weeded: 4

Note: 4 of the subjects whose biometrics are held due to a Wanted/Missing marker also have an ongoing investigation marker on file. However, until the outcome of that investigation is determined, the Wanted/Missing marker trumps the ongoing investigation marker in terms of biometric retention.

10.5 Despite the proportion of U18's being over 50% less than the O18's in respect of this data set, it is clear that the subjects who were under 18 at the time of arrest which resulted in the s.63G application are more likely to come to notice again based on this data. Out of the 126 data set of U18's, the 66 subjects came to notice again which represents a percentage of 52%[11].

10.6 Of the 47 U18's who came to notice again and were subject of an approved application, 14 subjects have been arrested 10 or more times since the s.63G application was made. Interestingly, the offences for which these subjects had a s.63G application made were in respect of similar offences, Robbery, Assault and Arson. The alleged offences that they then went on to commit followed a similar pattern in that they consisted of a variety of alleged offences related to burglary, criminal damage, assault and drugs.

Year of decision	Outcome	Age at time of arrest	s.63G offence	Similar or same alleged offence to s.63G?	Change	New status
2014	Approved	17	Robbery	Y	Y	Indefinite
2014	Approved	15	Robbery	Y	Y	Indefinite
2014	Rejected	15	Burglary and Theft - Non-Dwelling	Y	Y	Indefinite
2014	Approved	15	Wounding W/I To Do GBH	Y	Y	Indefinite
2014	Approved	14	AOABH	Y	Y	Impending
2015	Rejected	14	Rape of Female Under 16	N	Y	Indefinite
2015	Approved	16	Robbery	Y	Y	Indefinite
2015	Approved	16	Rape of Female Aged 16 Years Or Over	N	Y	Indefinite
2015	Approved	16	Wounding W/I To Do GBH	N	Y	Indefinite
2015	Approved	15	Causing Grievous Bodily Harm W/I To Do GBH	Y	Y	Indefinite
2016	Rejected	15	Burglary and Theft - Dwelling	Y	Y	Indefinite
2016	Approved	12	Arson	Y	Y	Indefinite
2016	Approved	14	AOABH	N	Y	Indefinite
2017	Approved	14	Arson	N	Y	Indefinite

[11] Whereas the 79 individuals who have come to notice again, out of the 261 data set who were over 18, represent a percentage of 30%.

11 Sexual Offences

11.1 Sex offences make up a large proportion of s.63G applications made by forces to the OBC and so, this specific category of alleged offending was looked at in more detail during this research.

11.2 238 of the 387 s.63G applications made to the OBC were in respect of a sexual offence as defined in the Sexual Offences Act 2003[12]. This represents 61% of the applications made during the aforementioned time frame.

11.3 171 subjects were **18 years or over** at the time of their arrest for an alleged sexual offence which resulted in the s.63G application.

11.4 Of the 171, 35 individuals came to police notice again and of those 35, 18 individuals have come to notice again for a further alleged sexual offence. An overview in respect of their biometric status is below but a complete breakdown of this data can be found at Annex E.

Over 18 Subject	Outcome of s.63G application	Total arrests on record	Number of arrests since s.63G	Biometric status
1	Approved	6	3	Indefinite
2	Rejected	9	8	Indefinite
3	Rejected	3	1	Weeded
4	Approved	4	1	Impending
5	Approved	6	4	Impending
6	Approved	3	1	Weeded
7	Approved	8	3	Impending
8	Approved	3	1	Indefinite
9	Rejected	2	1	Weeded
10	Rejected	2	1	Weeded
11	Rejected	3	1	Indefinite
12	Approved	3	1	Weeded
13	Approved	3	2	2 Years
14	Approved	2	1	Weeded
15	Approved	3	2	Indefinite
16	Approved	4	1	Indefinite
17	Approved	2	1	Weeded
18	Approved	2	1	Wanted Missing

11.5 67 of the subjects were **under the age of 18** at the time of their arrest.

11.6 Of the 67, 25 of the subjects have come to police notice again and 9 of those individuals have come to police notice for a further alleged sexual offence. A complete breakdown of this can be found at Annex F however, the table below just provides a summary in respect of the current position since the U18 was subject of a s.63G application.

[12] https://www.legislation.gov.uk/ukpga/2003/42/section/67

Under 18 Subject	Outcome of s.63G application	Total arrests on record	Number of arrests since s.63G	Biometric status
1	Rejected	13	12	Indefinite
2	Rejected	2	1	Weeded
3	Rejected	2	1	Impending
4	Rejected	2	1	Impending
5	Approved	2	1	WM Entry
6	Approved	2	1	Indefinite
7	Approved	3	2	3 Years
8	Approved	3	2	Weeded
9	Approved	5	2	Impending

11.1 The table at Annex F indicates that potentially 3 of the under 18 subjects came to notice for a more severe alleged sexual offence than that which led to the s.63G application which indicates a potential escalation in behaviour.

11.2 One category of sex offence which is of interest to the OBC are those where the victim is a child family member. This is because where the offence is amongst family members the subject is identifiable. Unless there is something which indicates that there is potential for offending outside the family, there is a lesser case for arguing why retention of biometrics would be useful as the subject is known.

11.3 In respect of the complete 387 data set, I identified five cases in respect of this for one of the following offences:

Incite Female Child Family Member Aged 13 - 17 Offender 18 Or Over To Engage in Sexual Act No Penetration
Sexual Activity With Female Child Family Member Under 13 - Offender 18 Or Over- No Penetration
Sexual Activity With Female Child Family Member 13 to 17
Sexual Activity With Female Child Family Member Under 13 - Offender 18 Or Over- No Penetration

11.4 However, I must note that the s.63G process deals with a much higher number of cases than 5 which relate to sex offences involving a family member however they are recorded under the more general offence titles of 'Rape' or 'Sexual Assault'. Without interrogating each application individually, I was unable to identify these additional cases due to time constraints however, this could be an area for further analysis.

11.5 However, the position in respect of these 5 cases is summarised in the table below. In all instances, the individual has not come to further notice since and their biometrics have fallen to automatic destruction.

Year of decision	Date of Arrest	Age at time of arrest	Outcome of s.63G	Arrest since s.63G?	Biometric status
2014	04/12/2013	33	Approved	No	Weeded
2016	10/09/2015	18	Rejected	No	Weeded
2016	09/05/2015	44	Rejected	No	Weeded
2016	26/02/2015	17	Approved	No	Weeded
2016	08/01/2015	16	Approved	No	Weeded

12 Previous Police Notice

12.1 One of the important considerations made during the s.63G decision process is whether the individual has previously come to police notice for certain offences which indicates that the individual poses a risk or whether they are a prolific offender for a certain type of alleged offence similar to that subject of the s.63G application.

12.2 A brief analysis was also conducted in respect of those individuals who had been subject of police notice prior to the s.63G application and whether any arrests were for an alleged offence which was of a similar nature to that subject of the s.63G application.

12.3 Of the 387 valid applications decided upon, 197 of the subjects had come to police notice before the s.63G application was made and is broken down as follows:

Subjects who had an arrest event prior to s.63G	Approvals	Rejections
197	161	36
Subjects who had an arrest event for a similar offence	Approvals	Rejections
120	102	18

12.4 As the table above indicates, 18 individuals who were refused had come to police notice prior to the arrest which resulted in the s.63G application. In respect of subsequent police notice following the refusal of the s.63G application, 11 of those subjects have not come to police notice since then.

12.5 However, the remaining 7 individuals did and a full breakdown of this can be found in Annex G.

12.6 It is clear that three of the subjects are classed as 'prolific offenders' given the amount of times that they have come to police notice since the event that they were arrested for which then resulted in the s.63G application. Whilst a decision to not retain the biometric material for 3 years in respect of the offence subject of the s.63G application was made, all three have since been convicted which means that their fingerprints and DNA will now be retained indefinitely in accordance with provisions contained in PoFA.

13 Comparative Analysis

13.1 A short piece of analysis was also conducted in respect of the most frequent alleged offences for which s.63G applications were made. The original intention was that this analysis would be in respect of the following four offences:

Offence 1 = Rape of Female Aged 16 Years or Over

Offence 2 = Robbery
Offence 3 = Sexual Assault – Intentionally Touch Female – No Penetration
Offence 4 = Causing Grievous Bodily Harm With Intent To Do Grievous Bodily Harm

Alleged offence	Under 18	Over 18	Total
Rape of Female Aged 16 Years Or Over	7	43	50
Robbery	26	20	46
Sexual Assault - Intentionally Touch Female - No Penetration	10	40	50
Causing Grievous Bodily Harm With Intent to Do Grievous Bodily Harm	8	12	20

13.2 It is clear that in respect of the U18 age categories, the prominent alleged offence is Robbery and whilst the other three offences are much lower in terms of numbers they still represent the next three frequent alleged offences for which a s.63G application was made during the specified time frame.

13.3 After collectively identifying the top alleged offences for which a s.63G application was made, for which the breakdown is above, I went through those records to determine where the majority of the age of the subjects sat in respect of the U18 and the O18 categories.

13.4 This is because QUEST searching on PNC provides for specific age categories in sets of 5 years as follows: 10-14, 15-19, 20-24, 25-29, 30-34 and so on.

13.5 The O18's age ranges breakdown as follows:

Alleged offence	18-19	20-24	25-29	30-34	35-39	40-44	45-49	50-54	55-59	60-64	65-69	70-74	75-79
Rape	5	5	11	8	4	3	2	4	1				
Robbery	9	6	2	1	2								
Sexual Assault	3	3	8	4	3	6	5	2	1	1		3	1
Causing GBH	1	4	2	3		1						1	

13.6 The U18's age ranges breakdown as follows:

Alleged offence	10-14	15-17
Rape	0	7
Robbery	3	23
Sexual Assault	4	6
Causing GBH	2	6

13.7 In respect of the O18's, the following searches were requested:

Offence: Robbery (Code: 5.1.1.1)
Age Range: 20:24
Gender: Male

Offence: Sexual Assault – Intentionally Touch Female – No Penetration (Code: 2.8.16.1)
Age Range: 20-24 and 25-29
Gender: Male

Offence: Sexual Assault – Intentionally Touch Female – No Penetration (Code: 2.8.16.1)
Age Range: 40-44 and 45-49
Gender: Male

Offence: Rape of a Female Aged 16 Years Or Over (Code: 2.1.4.2)
Age Range: 25-29 and 30-34
Gender: Male

Offence: Causing GBH With Intent to do GBH (Code: 1.9.8.1)
Age Range: 20-24 and 30-34
Gender: Male

13.8 In order to narrow down the number of hits in respect of each search, the search included the parameter of 'male' for the simple reason that males make up 97% of the s.63G applications analysed in this report.

13.9 Unfortunately though, each age category run against the offence code exceeded the maximum number of hits (over 2000 records) and therefore it was simply not possible to elicit date from these O18 searches.

13.10 Similar searches were also conducted in respect of the U18 age ranges. On this occasion, only two searches produced a list of hits which enabled me to interrogate records which I selected at random.

Search 1 - Offence: Robbery
Age Range: 10:14 (533 Hits)
Gender: Male

Search 2 - Offence: Sexual Assault – Intentionally Touch Female – No Penetration
Age Range: 10:14 (104 Hits)
Gender: Male

13.11 The return in respect of each search exceeded 100 records and therefore, this analysis was extremely small. I selected 30 records from each return at random to review.

13.12 I quickly realised that another problem with the QUEST search is that I was also not able to conduct a search solely on disposal and therefore, to find a record with a 'No Further Action' (NFA) outcome in respect of the alleged offence was going to be a lottery.

13.13 Whilst there are clear flaws with this method of searching, I decided to continue with an analysis anyway to just see whether, since the arrest for an offence listed above, that individual has come to notice again and if they have, whether the new alleged offence was more serious in nature and what the impact was upon the retention of their fingerprints and DNA.

13.14 None of the subject's records selected had been subject of a s.63G application.

13.15 The outcome for Search 1 is outlined below:

Biometric retention status	Totals
Indefinite	15
Impending	6
Specific Date	4
Not Held - Auto Weeded	5

13.16 What this indicates is that there were 5 records where the U18 individual was arrested and given an NFA for Robbery and there were no previous or subsequent events on their PNC record that was keeping the biometrics on. Therefore, the force could have considered making a s.63G application in respect of those individuals if they were so minded.

13.17 However, PNC does not record why a case was disposed of with an NFA and so there could be perfectly reasonable explanations as to why no application was made.

13.18 What the above also indicates is that a large proportion of the records already had indefinite retention or a specified time period applied to the retention of the biometrics and thus would not be eligible in respect of a s.63G application.

13.19 In respect of Search 2, similar to above, there was no particular cause for concern identified in respect of missed opportunities for making an application. Both were records owned by a force who does utilise the s.63G process and there were no other events on the record.

Biometric retention status	Totals
Indefinite	9
Impending	11
Specific Date	3
Not Held - Auto Weeded	2
Not Taken / Missing	5

13.20 In conclusion, due to the limitations of the QUEST search function on PNC, it was not possible to elicit a meaningful data set on this occasion. Perhaps this could be an area of research to develop in the future through whilst bearing in mind the functionality which might be introduced with the Law Enforcement Database System (LEDS).

14 Withdrawn Applications

14.1 Although withdrawn applications were out of scope of the main research conducted in respect of this report, a small review of such applications from the same time period was reviewed to determine whether the decision made by the force to withdraw the application was the correct one or whether the subject in question went on to come to police notice again and if so, for what sort of offences.

14.2 During the same time frame applied to the data in this report, the OBC received a total of 49 withdrawn applications.

14.3 The reasoning behind the withdrawal of a s.63G application includes the following:

14.3.1 The record already had indefinite retention of biometrics applied so an application was not needed as biometric retention was already lawful.

14.3.2 The force neglected to put the relevant marker on the PNC record causing the biometric material to weed.

14.3.3 The application was outside of the time frame.

14.4 The breakdown of the 49 withdrawn applications is outlined below:

Subsequent police notice	Totals
Has not come to police notice	16
Has come to police for non-qualifying offence	7
Has come to police notice for qualifying offence	26
Total Withdrawn Applications	49

14.5 21 of the 26 subjects who came to police notice again for a Qualifying Offence have had indefinite retention applied to their fingerprints and DNA as a resulted of having being convicted since the arrest which initiated the s.63G application or because they already had a conviction resulting in indefinite retention which was why the s.63G application was withdrawn.

14.6 There are 3 subjects who were arrested for an alleged sex offence which then triggered the s.63G application.

14.7 2 came to notice again for a further alleged sex offence which was also disposed of by a No Further Action (NFA). As a result, the fingerprints and DNA fell to automatic weeding. These could be viewed as missed opportunities for submitting a further s.63G application however, without the knowledge of the cases and the reasoning as to why the cases were NFA'd, this cannot be determined for sure.

14.8 Furthermore, whilst the force might have considered making a second s.63G application in respect of the second alleged sex offence that the subject was arrested for, it is of note that that there have been no arrests for these two subjects since 2013 or 2015 respectively.

14.9 In respect of the third subject, they were arrested for a further two alleged sex offences in 2014 and 2017. One of the arrests resulted in a charge and as the subject was found not guilty, a three year retention was applied to the fingerprints and DNA from the date the samples were taken. They have since fallen to automatic deletion but as the individual was arrested, charged but not convicted of a Qualifying Offence the event was not eligible under the s.63G process.

14.10 A full overview of the findings in respect of withdrawn applications can be found in Annex H.

15 DNA Hits

15.1 A final area of analysis which was conducted was in respect of the DNA still held against an individual and which was taken in respect of the arrest which resulted in the s.63G application.

15.2 122 DNA barcodes were submitted to the National DNA Database (NDNAD) to ascertain whether the DNA profile resulted in a match against a crime scene mark and for what offence that crime scene mark was in relation to.[13]

15.3 The barcodes which were sent were only in relation to DNA profiles which were taken in respect of the arrest which resulted in the s.63G application and were still being retained on the NDNAD.

15.4 119 of the profiles belonged to individuals who had been subject of an approved s.63G application. 3 had been the subject of a rejected s.63G application but soon after (within less than a year in all 3 cases) the decision of the OBC those individuals had been arrested and convicted of a different offence which resulted in the indefinite retention of their biometrics anyway.

15.5 In instances where the DNA taken in respect of the arrest which generated the s.63G application but the PNC record confirmed that the material had been destroyed (due to the expiry of the three year period), there was often no DNA barcode recorded on the record because the profile had been deleted from the database.

15.6 The data returned indicated that twenty four matches were identified against crime scene marks held within the NDNAD in respect of seventeen subjects. As the table in Annex I indicates, five subjects had a hit against more than one crime scene mark.

15.7 Column B states the alleged offence or offences for which a DNA match was made against a crime scene mark. As a comparison, the alleged offence subject of the s.63G application is listed at Column C.

15.8 One subject, who was arrested for a sexual assault in respect of the s.63G application, had a DNA hit against an offence of Rape and it is such scenarios where the value of biometrics really demonstrates its importance if behaviour of a certain nature is seen to escalate.

15.9 When the NDNAD identify a match, a match report is automatically generated and sent to the force that owns the sample and the force that owns the crime scene sample. It is then the responsibility of the force that owns the crime scene sample to act upon that match.

15.10 In many instances, there is no record of arrest in respect of the crime scene mark on the PNC record of the individual concerned which is represented in Column D. However, this is not too concerning as the biometrics for all of the seventeen subjects are held either indefinitely or due to an approved s.63G application.

15.11 Where there is a 'maybe' this is because whilst there is an offence of the same title as the offence that was matched that is recorded on the individuals PNC record, without a date it cannot be determined for sure as to whether that specific event was recorded as a result of the DNA hit. However, this could be an area for development for future research.

[13] Many thanks to the National DNA Database for providing this data.

16 Round Up

16.1 The data set reviewed as part of this report was vast and varied. A great deal of analysis has been undertaken in respect of the data and various variables have been looked at to ascertain as to whether there are any clear patterns that have emerged.

16.2 These include a review of the following areas:

- The data set as a whole in terms of the ratio of approvals and rejections.
- The data set as whole in terms of those who came to police notice again and those who did not, for what sorts of offences and whether there was an impact on biometric retention.
- The data set specifically in terms of applications which were approved / rejected and those who came to police again, arrest volumes and impact on biometric retention.
- A general overview specifically in respect of applications for individuals who were 18 years or over at the time of the arrest which resulted in the s.63G application, subsequent police notice and the impact on biometric retention.
- A general overview specifically in respect of applications for individuals who under the age of 18 years or over at the time of the arrest which resulted in the s.63G application, subsequent police notice and the impact on biometric retention.
- A specific focus on sex offences subject of the s.63G process in respect of both the U18 and 18 or over age categories, subsequent police notice and the impact on biometric retention.
- A review of previous police notice prior to the arrest resulting in the s.63G application.
- A small comparative analysis in respect of the top two offences submitted under the s.63G process in respect of under 18's to identify any potential missed opportunities.
- A review of the withdrawn applications and the subsequent police notice to ascertain whether there were any potential missed opportunities.
- Review of the DNA hits in respect of profiles held in respect of the arrest resulting in the s.63G process to determine how many hits were made against crime scene marks.

16.3 In terms of findings, I've outlined below a summary of the main figures identified in this report which might be of interest.

16.4 The Metropolitan Police Service (MPS) represent 74% of the total s.63G applications made by forces across England and Wales during the time frame selected for this research. This is not unsurprising given that they cover the largest geographical area. 215 of the applications that they submitted were approved and 70 applications were rejected.

16.5 The approval rate of the applications reviewed as part of the 387 data set also equated to 74% and therefore, this indicates that three quarters of the applications submitted to the OBC by forces are seen to be justified and proportionate and that, in the large, the correct individuals are being put forward to have their biometrics retained.

16.6 Of the 288 approval decisions made, 118 individuals came to police notice again following the arrest which resulted in the s.63G application. This represents 41% of subjects and therefore, it indicates that simply being the subject of such an application does not necessarily act as a preventative measure.

16.7 However, by looking at both the approved applications and the rejected applications combined, 145 individuals came to police notice which represents a lower proportion of 37% against the total data set of 387 applications.

16.8 In terms of refused applications, out of the 99 subjects, just 27 came to police notice again which, is potentially reassuring given the low volume.

16.9 In respect of subjects who were 18 years or over, just 30% came to police notice again. In respect of subjects who were under the age of 18 at the time of their arrest, 52% came to police notice again.

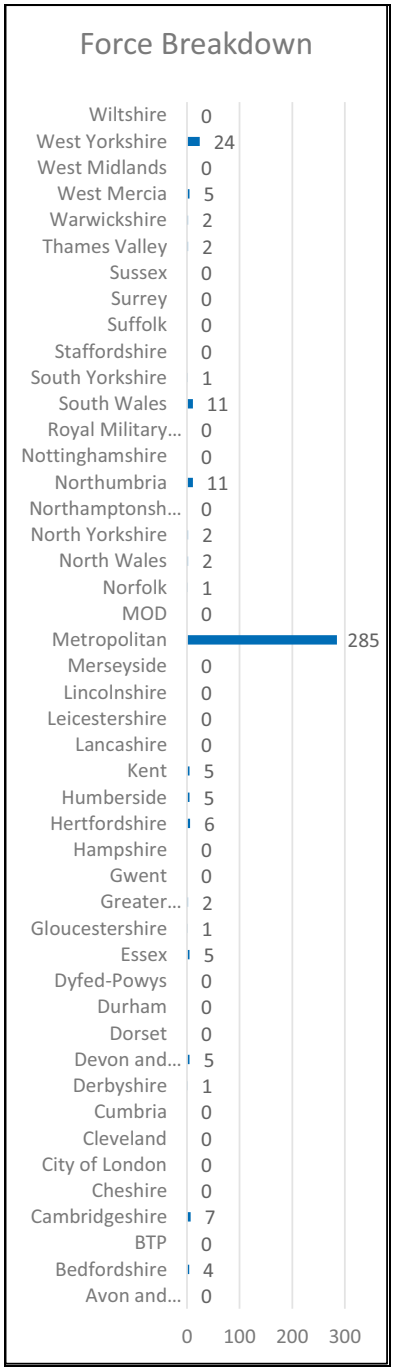
16.10 Although, the proportion of O18 v U18 is different, with 261 of the s.63G applications being in respect of an O18 and 126 being in respect of an U18, the above indicates that an U18 is more likely to come to notice again.

16.11 Sex offences represent 61% of the alleged offences for which a s.63G application is made by forces – this represents 238 applications out of the total 387 reviewed in this report.

16.12 171 subjects were 18 years or over at the time of their arrest (72%) for an alleged sex offence, 35 individuals came to police notice again and of those 35, 18 individuals have come to notice again for a further alleged sexual offence.

16.13 67 individuals were under the age of 18 at the time of their arrest (28%) for an alleged sex offence, 25 of the subjects have come to police notice again and 9 of those individuals have come to police notice for a further alleged sexual offence.

Annex A – Force breakdown of s.63G application submissions



Force	Approvals	O18	U18	Rejections	O18	U18
2	215	147	68	70	30	40
6	2	2	0	0	0	0
10	8	8	0	3	2	1
12	2	2	0	0	0	0
13	23	15	8	1	1	0
14	1	0	1	0	0	0
16	3	2	1	2	1	1
22	2	2	0	3	2	1
23	0	0	0	2	1	1
30	1	1	0	0	0	0
35	4	4	0	3	3	0
36	0	0	0	1	1	0
40	4	3	1	0	0	0
41	3	2	1	3	0	3
42	1	1	0	4	4	0
43	2	2	0	0	0	0
46	4	2	2	1	1	0
50	5	3	2	0	0	0
53	1	1	0	0	0	0
60	2	1	1	0	0	0
62	5	3	2	6	4	2

Data accurate and representative as of 08/11/2018
Only represents applications submitted from 31/10/2013 – 08/11/2017

Annex B – Arrest information post s.63G application submission

Subject came to police notice post the arrest resulting in s.63G application – yes/no

Year	Yes	No
2014	26	20
2015	38	47
2016	56	120
2017	25	55
TOTALS	145	242

Note 1: No applications were submitted to the OBC in 2013.
Note 2: Information elicited from the Police National Computer (PNC) between 08/11/2018 – 29/11/2018.

Table 1 - Of those which were a 'yes' how many have been subject of 1-5 arrests since s.63G application?

Year	Total	Approved	O18	Biometric Status		U18	Biometric Status		Rejected	O18	Biometric Status		U18	Biometric Status	
2014	**17**	**16**	14	5	ID	2	2	ID	**1**	1	1	ID	0	N/A	
				1	IP										
				8	BW										
2015	**28**	**24**	21	8	ID	3	1	ID	**4**	2	2	BW	2	1	ID
				4	IP		1	IP						1	BW
				9	BW		1	BW							
2016	**47**	**33**	22	7	ID	11	5	ID	**14**	3	1	ID	11	2	ID
				1	IP		2	WM			2	BW		2	IP
				10	BW		3	BW						6	BW
				2	WM		1	TY						1	WM
2017	**24**	**21**	8	4	ID	13	5	ID	**3**	1	1	ID	2	1	IP
				1	IP		3	IP						1	BW
				3	WM		5	WM							
	116														

Table 2 - Of those which were a 'yes' how many have been subject of 6-9 arrests since s.63G application?

Year	Total	Approved	O18	Biometric Status		U18	Biometric Status		Rejected	O18	Biometric Status		U18	Biometric Status	
2014	**3**	**1**	1	1	ID	0	N/A		**2**	1	1	ID	1	1	ID
2015	**4**	**4**	0	N/A		4	3	ID	**0**	0	N/A		0	N/A	
							1	IP							
2016	**6**	**6**	3	3	ID	3	2	ID	**0**	0	N/A		0	N/A	
							1	WM							
2017	**0**	**0**	0	N/A		0	N/A		**0**	0	N/A		0	N/A	
	13														

Table 3 - Of those which were a 'yes' how many have been subject of 10+ arrests since s.63G application?

Year	Total	Approved	O18	Biometric Status		U18	Biometric Status		Rejected	O18	Biometric Status		U18	Biometric Status	
2014	**6**	**5**	1	1	ID	4	3	ID	**1**	0	N/A		1	1	ID
							1	IP							
2015	**6**	**5**	1	1	ID	4	4	ID	**1**	0	N/A		1	1	ID
2016	**3**	**2**	0	N/A		2	2	ID	**1**	0	N/A		1	1	ID
2017	**1**	**1**	0	N/A		1	1	ID	**0**	0	N/A		0	N/A	
	16														

Table 4 - Those subject to no arrests since s.63G application.

Year	Total	Approved	O18	Biometric Status		U18	Biometric Status		Rejected	O18	Biometric Status		U18	Biometric Status	
2014	**20**	**17**	17	17	BW	0	N/A		**3**	3	3	BW	0	N/A	
2015	**47**	**35**	30	30	BW	5	5	BW	**12**	11	11	BW	1	1	BW
2016	**120**	**77**	53	32	BW	24	19	BW	**43**	29	29	BW	14	14	BW
				21	WM		5	WM							
2017	**55**	**41**	30	2	BW	11	11	WM	**14**	10	10	BW	4	4	BW
				28	WM										
	242														

Key	
Indefinite	ID
Impending	IP
Biometrics Weeded	BW
Wanted/Missing marker (specifically UZ)	WM
Further three years*	TY
Two years	PND

***arrested charged but not convicted of a Qualifying Offence.**

Annex C – Approvals and arrest overlap data

Date of s.63G arrest	Date of decision	New event date amending retention	Outcome	Within 3 year timeframe
01/04/2014	05/11/2014	03/02/2015 and 26/06/2018	Arrested Charged Not Convicted of QO then Caution	Yes
04/04/2014	18/08/2014	10/10/2016	Court Conviction	Yes
28/02/2014	05/11/2014	22/11/2018	Impending	No
22/11/2013	28/03/2014	11/02/2016	Court Conviction	Yes
20/02/2014	15/07/2014	16/02/2015	Court Conviction	Yes
15/01/2014	08/08/2014	24/05/2014	Youth Caution	Yes
01/04/2014	05/11/2014	02/11/2015	Court Conviction	Yes
31/01/2014	03/12/2014	18/09/2015	Court Conviction	Yes
31/01/2014	15/07/2014	06/09/2018	Impending	No
30/03/2014	08/08/2014	19/10/2015	Caution	Yes
06/04/2014	12/08/2014	20/08/2014	Conditional Caution	Yes
26/02/2014	12/08/2014	19/01/2015	Court Conviction	Yes
04/01/2014	21/08/2014	31/08/2016	Court Conviction	Yes
21/03/2014	17/12/2014	22/01/2016	Court Conviction	Yes
15/02/2014	06/02/2015	06/06/2016	Impending	Yes
03/06/2014	10/08/2015	07/10/2018	Impending	No
17/05/2014	21/01/2015	12/03/2015	Court Conviction	Yes
06/05/2014	03/02/2015	14/07/2014	Court Conviction	Yes
15/02/2014	06/02/2015	24/01/2017	Caution	No
19/07/2014	24/08/2015	04/02/2016	Court Conviction	Yes
15/08/2014	28/08/2015	25/09/2018	Impending	No
23/09/2014	21/08/2015	21/10/2015	Court Conviction	Yes
16/02/2014	04/03/2015	14/05/2017	Impending	No
02/06/2014	11/03/2015	01/05/2018	Impending	No
13/06/2014	13/04/2015	31/05/2018	Court Conviction	No
15/02/2014	20/04/2015	31/08/2014	Court Conviction	Yes
30/07/2014	23/04/2015	07/07/2016	Caution	Yes
05/12/2013	29/04/2015	22/05/2015	Court Conviction	Yes
02/07/2014	06/05/2015	12/12/2015	Court Conviction	Yes
11/07/2014	18/05/2015	20/01/2016	Court Conviction	Yes
26/07/2014	20/05/2015	05/06/2017	Caution	Yes
16/09/2014	27/05/2015	26/10/2017	Caution	Yes
02/05/2014	29/06/2015	29/08/2018	Impending	No
04/10/2014	01/07/2015	07/03/2015	Court Conviction	Yes
23/04/2014	26/06/2015	04/02/2016	Court Conviction	Yes
25/08/2014	04/08/2015	22/06/2016	Court Conviction	Yes
07/11/2013	04/08/2015	18/12/2018	Caution	No
26/02/2015	28/06/2016	09/08/2016	Conditional Caution	Yes
06/09/2015	19/07/2016	22/07/2018	Court Conviction	No
21/07/2015	23/08/2016	16/06/2016	Court Conviction	Yes
25/09/2015	22/06/2016	27/10/2016	PND	Yes
04/02/2016	20/09/2016	14/05/2017	Court Conviction	Yes
09/12/2014	08/01/2016	21/11/2017	Court Conviction	Yes
20/06/2014	02/02/2016	07/06/2015	Conditional Caution	Yes
16/12/2013	22/01/2016	30/01/2017	Court Conviction	No
14/02/2015	22/01/2016	03/03/2016	Court Conviction	Yes
25/09/2014	02/02/2016	14/10/2016	Court Conviction	Yes
01/04/2014	01/02/2016	16/08/2016	Court Conviction	Yes
02/01/2016	07/09/2016	26/10/2016	Court Conviction	Yes
17/04/2016	05/10/2016	21/06/2016	Court Conviction	Yes
29/01/2015	05/10/2016	15/09/2016	Court Conviction	Yes
19/09/2015	04/11/2016	01/12/2016	PND	Yes
24/05/2015	22/06/2016	09/04/2017	Arrested Charged Not Convicted of QO	Yes
02/06/2015	02/03/2016	15/02/2016	Youth Caution	Yes
24/06/2015	20/06/2016	07/01/2017	Court Conviction	Yes
17/07/2015	18/07/2016	16/11/2015	Impending	Yes
17/09/2015	06/07/2016	28/06/2018	Court Conviction	Yes
13/11/2015	23/08/2016	29/09/2016	Court Conviction	Yes
03/11/2015	22/08/2016	25/08/2018	Court Conviction	Yes
30/05/2016	13/01/2017	03/04/2018	Court Conviction	Yes
12/09/2016	19/04/2017	18/09/2016	Court Conviction	Yes
29/11/2016	13/04/2017	10/08/2017	Court Conviction	Yes
10/06/2016	10/05/2017	18/06/2018	Impending	Yes
19/03/2017	26/06/2017	22/08/2018	Impending	Yes
21/10/2016	29/06/2017	21/11/2017	Conditional Caution	Yes
24/02/2017	11/08/2017	05/04/2018	Court Conviction	Yes
23/01/2015	19/01/2017	07/09/2018	Impending	Yes
14/09/2015	13/04/2017	03/02/2018	Impending	Yes
20/03/2016	11/08/2017	30/03/2016	Court Conviction	Yes
06/06/2016	29/06/2017	01/01/2017	Court Conviction	Yes
06/01/2017	27/07/2017	16/04/2017	Court Conviction	Yes
07/10/2016	10/05/2017	13/09/2017	Court Conviction	Yes
20/06/2017	02/11/2017	08/09/2017	Court Conviction	Yes

Annex D – Refused applications and subsequent arrest

Offence subject of s.63G	Arrested for a similar alleged offence post s.63G	Arrested for an alleged qualifying offence post s.63G	Alleged offence	Court conviction	Caution	Biometric status	Arrest date	Age at time of s.63G arrest
Exposure	Y	Y	Exposure	Y	N	Indefinite	16/11/2013	85
Rape of Female Aged 16 Years Or Over	N	N	Breach of non molestation order	N	Y	Indefinite	27/12/2013	41
Wounding / Inflicting GBH	N	Y	Rape A Girl U13	N	N	Indefinite	19/03/2014	16
Burglary and Theft - Non-Dwelling	Y	Y	Aggravated Burglary (Comprising Commission of Offence - Burglary)	N	N	Indefinite	04/03/2014	15
Rape of Female Under 16	Y	Y	Rape a Girl U13	N	N	Indefinite	06/02/2014	14
Sexual Assault - Intentionally Touch Female - No Penetration	N	N	Non Patrial Overstaying Leave	N	N	Now Weeded	14/04/2014	22
Rape A Girl U13	Y	Y	Rape of Female Aged 16 Years Or Over	N	N	Now Weeded	12/11/2013	24
Burglary and Theft - Dwelling	N	Y	AOABH	N	N	Now Weeded	11/07/2014	15
Sexual Assault on Female By Penetration	N	N	Battery	N	Y	Indefinite	22/02/2015	16
Rape of Female U16	N	N	Dangerous Driving	Y	N	Indefinite	28/02/2014	13
Assault Female Child U13 - Penetration of Vagina / Anus With Part of Body / Object	Y	Y	Assault Female Child U13 - Penetration of Vagina / Anus With Part of Body /Object	N	N	Now Weeded	02/10/2014	31
Sexual Assault - Intentionally Touch Male - No Penetration	Y	Y	Sexual Activity with Female Child Family Member U13 - Offender O18	N	N	Wanted/Missing	25/02/2015	10
Sexual Assault - Intentionally Touch Female	N	N	Possess Controlled Drug - Class B - Cannabis/Resin	N	N	Now Weeded	07/08/2014	14
Rape of Female U16	Y	Y	Rape of Female Aged 16 Years Or Over	N	N	Now Weeded	29/07/2014	20
Rape of a Boy U13	N	Y	Robbery	N	N	Now Weeded	31/07/2014	13
Causing Grievous Bodily Harm W/I To Do GBH	Y	N	Violent Disorder	N	N	Now Weeded	04/11/2014	12
Burglary and Theft - Dwelling	Y	Y	Burglary and Theft - Dwelling	N	Y	Indefinite	06/07/2015	15
Rape of a Boy U13	N	N	Possess Controlled Drug - Class B - Cannabis/Resin	N	Y	Indefinite	23/11/2014	12
Rape of a Boy U13	Y	Y	Rape of a Boy U13 - NFA	N	N	Now Weeded	20/08/2014	13
Rape of Female U16	N	N	Possess Controlled Drug - Class B - Cannabis/Resin	N	N	Now Weeded	06/06/2014	15
Sexual Assault of Female Child U13 (x3 Counts)	Y	Y	Rape of Female U16	Impending	Impending	Impending	03/07/2015	13
Causing Grievous Bodily Harm W/I To Do GBH	N	N	Possess Controlled Drug - Class B - Cannabis/Resin	N	N	Now Weeded	12/11/2015	15
Taking Indecent Photographs Or Pseudo-Photographs of Children	Y	Y	Sexual Assault - Intentionally Touch Female - No Penetration	Impending	Impending	Impending	30/01/2016	12
Rape of Female Aged 16 Years Or Over	Y	Y	Sexual Assault - Intentionally Touch Female - No Penetration	Y	N	Indefinite	11/04/2016	44
Sexual Activity With Male Child U13 - Offender Aged U18 - No Penetration	N	N	Theft of Vehicle	N	N	Impending	14/07/2016	12
Possess To Show/Distribute Indecent Photograph/Pseudo Photograph Of A Child	N	N	Send Communication/Article Of An Indecent/Offensive Nature	N	N	Now Weeded	26/04/2016	16
Robbery	N	N	Send Communication/Article Of An Indecent/Offensive Nature	N	Y	Indefinite	19/10/2016	18

This table represents the 27 subjects who were subject of a refused application submitted under s.63G of PACE and who came to subsequent police

Annex E – Over 18 – Alleged sexual offences and subsequent police notice

Subject	Alleged offence subject of s.63G application	New alleged offence(s) arrested for	Disposal	Outcome	Age at time of arrest	Age at time of new arrest(s)
Subject 1	Rape of Female Under 16	Breach of Interim Sexual Offences	Caution	Approved	28	28, 29 and 31
	Sexual Assault Intentionally Touch Female - No Penetrati	Sexual Activity With U16 Offender 18 Or Over (x4 Counts)	Not Guilty			
	Adult Meet Girl U16 Following Sexual Grooming	Sexual Activity Female Child U16 Offender 18 or Over	Not Guilty			
Subject 2	Exposure	Exposure	Guilty	Rejected	85	85 and 86
		Cause/Incite Female To Engage In Sexual Activity - Offender 18 Or Over	Guilty			
		Exposure (x2 counts)	Not Guilty			
		Sexual Assault - Intentionally Touch Female - No Penetration - Guilty	Guilty			
		Sexual Assault - Intentionally Touch Female - No Penetration (x2 counts)	Impending			
Subject 3	Rape A Girl U13	Rape of Female Aged 16 Years Or Over	NFA	Rejected	24	26
Subject 4	Sexual Assault of Male Child U13	Sexual Assault of Male Child U13	Impending	Approved	21	25
Subject 5	Sexual Activity With Female Child U16 - Offender 18 Or Over - No Penetration	Rape of Female Aged 16 Years Or Over	Impending	Approved	22	23 and 26
		Sexual Assault - Intentionally Touch Female - No Penetration	NFA			
Subject 6	Sexual Activity With Female Child U13	Offender 18 Or Over Engage in Penetrative Sexual Activity With Girl U13	NFA	Approved	29	30
Subject 7	Rape of Female Aged 16 Years Or Over	Rape of Female Aged 16 Years Or Over (x4 Counts)	Impending	Approved	31	32, 33 and 35
		Sexual Assault - Intentionally Touch Female - No Penetration	Impending			
		Rape of Female Aged 16 Years Or Over	NFA			
		Cause/Incite Prostitution for Gain	NFA			
		Control Prostitution for Gain	NFA			
Subject 8	Sexual Assault - Intentionally Touch Female - No Penetration	Sexual Assault - Intentionally Touch Female - No Penetration	Guilty	Approved	48	50
		At/Sexual Assault - Intentionally Touch Female - No Penetration	NFA			
Subject 9	Assault Female Child U13 - Penetration of Vagina / Anus With Part of Body /Object	Assault Female Child U13 - Penetration of Vagina / Anus With Part of Body / Object	NFA	Rejected	31	31
Subject 10	Rape of Female Under 16	Rape of Female Aged 16 Years Or Over	NFA	Rejected	20	21
Subject 11	Rape of Female Aged 16 Years Or Over	Sexual Assault - Intentionally Touch Female - No Penetration (x2 counts)	Guilty	Rejected	44	44
Subject 12	Rape of Female U16 AOABH	Sexual Activity Female Child U16 Offender 18 Or Over - Penetrate Anus/Vagina/Mouth	NFA	Approved	19	19
Subject 13	Rape of Female Aged 16 Years Or Over	Rape of Female Under 16	NFA	Approved	18	19
Subject 14	Rape of Female Aged 16 Years Or Over Sexual Assault on Female By Penetration	Making Indecent Photograph or Pseudo-Photograph of Children	NFA	Approved	31	31
Subject 15	Cause/Incite Female Child U16 To Engage in Sexual Activity - Offender 18 Or Over - No Penetration	Exposure	NFA	Approved	21	25
Subject 16	Sexual Assault - Intentionally Touch Male - No Penetration	At/Cause/Incite Female Child U16 To Engage in Sexual Activity - Offender 18 Or Over - No Penetration	Guilty	Approved	29	32
Subject 17	Sexual Assault - Intentionally Touch Female - No Penetration	Voyeurism - Operate Equipment To Enable Another to Observe a Private Act	NFA	Approved	28	29
Subject 18	Sexual Activity With Female Child U13 - Offender 18 Or Over - No Penetration	Sexual Assault - Intentionally Touch Female - No Penetration	Impending	Approved	36	36

Annex F – Under 18 – Alleged sexual offences and subsequent police notice

Subject	Alleged offence subject of s.63G application	New alleged offence(s) arrested for	Disposal	Outcome	Age at time of arrest	Age at time of new arrest(s)
Subject 1	Rape of Female Under 16	Rape of Girl Under 13	NFA	Rejected	14	18
Subject 2	Rape of a Boy U13 Distributing Images	Rape of a Boy Under 13	NFA	Rejected	13	13
		Distributing Indecent Photographs or Pseudo-Photographs of Children	NFA			
		Possess to Show/Distribute Indecent Photograph/Pseudo Photograph of a Child	NFA			
Subject 3	Sexual Assault of Female Child U13 (x3 Counts)	Rape of Female Under 16 (x3 Counts)	Impending	Rejected	13	16
		Arrange / Facilitate The Commission Of A Child Sex Offence	Impending			
		Distributing Indecent Photographs or Pseudo-Photographs Of Children	Impending			
Subject 4	Taking Indecent Photographs Or Pseudo-Photographs of Children	Sexual Assault - Intentionally Touch Female - No Penetration	Impending	Rejected	12	14
Subject 5	Rape A Girl U13	Possessing an Indecent Photograph or Pseudo-Photograph of A Child	NFA	Approved	12	13
Subject 6	Sexual Assault - Intentionally Touch Female - No Penetration	Assault Female Child U13 - Penetration of Vagina / Anus With Part of Body / Object - (X2 Counts)	Guilty - Unfit to Plead - Sexual Risk Order	Approved	14	15
		Sexual Assault Of Female Child U13 (x2 Counts)	Not Guilty			
Subject 7	Exposure	Exposure	Discontinuance	Approved	16	17
		Exposure	NFA			16
Subject 8	Rape A Girl U13	Possessing an Indecent Photograph or Pseudo-Photograph of A Child	NFA	Approved	15	15
		Rape of Female Aged 16 Years or Over (x4 Counts)	NFA			
Subject 9	Rape A Girl U13	Rape of Female Aged 16 Years Or Over (x2 Counts)	Impending	Approved	16	18
		Sexual Activity Female Child U16 Offender 18 Or Over - Penetration	NFA			

Annex G – Rejections – Previous police notice

Decision Date	Age at time of arrest	Total arrests on record	Alleged offence subject of s.63G application	Number of arrests since s.63G	Term of imprisonment since s.63G	Alteration to biometrics due to new arrest?	What is current biometric status?	Number of arrests since s.63G by category	Police notice for similar offence PRIOR to s.63G	Alleged offfence
28/02/2014	85	9	Exposure	8	Y	Y	Indefinite	6-9	Y	1) Sexual Assault - Intentionally Touch Female - No Penetration
20/11/2014	15	23	Burglary and Theft - Non-Dwelling	15	Y	Y	Indefinite	10+	Y	1) Robbery 2) Burglary
24/08/2015	15	6	Burglary and Theft - Dwelling	1	N	N	Bios now weeded	1-5	Y	1) Robbery 2) Theft of Vehicle 3) Going Equipped For Theft
14/01/2016	31	2	Assault Female Child U13	1	N	N	Bios now weeded	1-5	Y	1) Assault Female Child U13
18/07/2016	15	14	Burglary and Theft - Dwelling	11	N	Y	Indefinite	10+	Y	1) Theft - Shoplifting 2) Theft of Vehicle
03/08/2016	14	2	Rape of a Boy U13	1	N	N	Bios now weeded	1-5	Y	1) Rape of Male U16
20/02/2017	16	3	Possess To Show/Distribute Indecent Photograph/Pseudo Photograph Of A Child	1	N	N	Bios now weeded	1-5	Y	1) Distribute An Image Of A Child 2) Sexual Assault on Female

Annex H – Withdrawn applications breakdown

Age at time of arrest	Decision date	Alleged offence subject of s.63G Application	Come to notice for QO since?	New arrest date	Alleged offence	Outcome	Current biometric status
20	05/06/2014	Rape of Female Aged 16 Years Or Over	Y	27/03/2014	At/Cause/Incite Female Child U16 Engage Sexual Act Offender 18+ Penetrate Anus/Vagina/Mouth By Penis/Body Part	NFA	Indefinite
30	05/06/2014	AOABH	N	N/A	N/A	N/A	Weeded
14	05/06/2014	Wounding / Inflicting GBH	Y	11/08/2016	AOABH	Guilty	Indefinite
16	02/04/2014	Cause/Incite Male Child U13 To Engage In Sexual Act - Offender 18 Or Over - No Penetration	Y	19/12/2017 26/03/2014	Cause/Incite Female Child U16 To Engage in Sexual Activity - Offender 8 Or Over - No Penetration Sexual Assault of Male Child U13	NFA Not Guilty	Weeded
17	04/04/2014	AOABH	Y	03/04/2018	At/Wounding With Intent To Do GBH	Guilty	Indefinite
21	01/04/2014	Possess Firearm With Intent To Cause Fear Of Violence	N	Has come to notice for non QO and received a court conviction		Guilty	Indefinite
65	05/06/2014	Voyeurism - Operate Equipment To Enable Another To Observe A Person Doing A Private Act	N	Has come to notice for non QO and received a court conviction		NFA	Weeded
39	05/06/2014	Exposure	Y	29/11/2013	Public Nuisance - Indecent Exposure	NFA	Weeded
13	17/06/2014	Rape of Female Under 16	Y	06/03/2014	1) Robbery 2) At/Robbery	NFA	Indefinite
35	18/08/2014	Sexual Assault - Intentionally Touch Female - No Penetration	Y	19/11/2016	1) Sexual Activity With Female Child Under 16 - Offender 18 Or Over - No Penetration 2) Sexual Assault - Intentionally Touch Female - No Penetration	NFA Not Guilty	Three years from sample date (19/11/2019)
15	17/03/2015	Robbery	Y	18/09/2017	1) Wounding W/I To Do GBH 2) Causing GBH With Intent To Do GBH	Not Guilty Not Guilty	Indefinite
15	03/03/2015	Wounding W/I To Do GBH	Y	05/08/2017	Robbery	NFA	Indefinite
18	31/03/2015	Robbery	Y	21/03/2016 23/07/2015 24/10/2015 18/08/2014	Robbery Threats to Kill Causing GBH W/I To Do GBH Robbery	Not Guilty NFA NFA NFA	Indefinite
16	03/03/2015	Rape of Female Under 16	Y	17/11/2014 21/04/2014	Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Wounding/Inflicting GBH	Not Guilty NFA	Indefinite
14	25/02/2015	Wounding W/I To Do GBH	y	01/09/2015 10/08/2015 20/06/2015 04/04/2015 31/01/2015 04/11/2014 24/10/2014	AOABH Wounding / Inflicting GBH 1) Wounding/Inflicting GBH 2) AOABH 3) Wounding/Inflicting GBH Threats To Kill 1) Robbery 2) AOABH Making Indecent Photograph or Pseudo Photograph of Children AOABH	Not Guilty NFA NFA Withdrawn Final Guilty NFA Not Guilty NFA NFA NFA	Indefinite
18	13/01/2015	Wounding W/I To Do GBH	Y	29/01/2016 02/06/2015 25/08/2014	Threats to Kill Threats to Kill AOABH	NFA NFA NFA	Indefinite
17	24/11/2014	Cause/Incite A Girl Under 13 To Engage In Sexual Activity - No Penetration	N	N/A	N/A	N/A	Weeded
14	24/02/2014	Sexual Assault - Intentionally Touch Female - No Penetration	Y	04/05/2017	1) Assault A Female Child U13 - Penetration of Vagina/Anus With Part of Body/Object 2) Rape A Girl Under 13 (x6 Counts)	Guilty Guilty	Indefinite
17	02/09/2015	Robbery	Y	04/02/2016 19/01/2016 26/11/2015 12/07/2015 31/10/2014	Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Murder Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Cause/Incite Female Child U16 To Engage In Sexual Act Taking Indecent Photogaphs or Pseudo Photographs of Children Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Sexual Activity Female Child U16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Robbery	NFA NFA Not Guilty Not Guilty Guilty Lie on File NFA Not Guilty NFA	Indefinite
15	28/07/2015	Robbery	N	Has come to notice for non QO and received a court conviction		Guilty	Indefinite
28	13/03/2015	Sexual Assault - Intentionally Touch Female - No Penetration	Y	20/02/2015	Voyeurism - Operate Equipment to Enable Another To Observe A Person Doing A Private Act	NFA	Weeded
16	05/05/2015	Robbery	Y	21/03/2017 31/05/2015	C/Robbery AOABH	Guilty NFA	Indefinite
39	21/07/2015	Rape of Female Aged 16 Years Or Over	N	N/A	N/A	N/A	Weeded

Annex H – Withdrawn applications breakdown – continued

Age at time of arrest	Decision date	Alleged offence subject of s.63G Application	Come to notice for QO since?	New arrest date	Alleged offence
16	09/09/2015	Arson With Intent/Reckless As To Whether Life Was Endangered	Y	05/07/2015 26/05/2015 03/04/2015	AOABH 1) Sexual Assault - Intentionally Touch Female - No Penetration 2) Exposure Burglary and Theft - Non Dwelling
27	08/02/2016	Wounding/Inflicting GBH	N	N/A	N/A
12	06/10/2015	Robbery	Y	15/03/2018 17/01/2018 01/11/2015 09/09/2015 12/08/2015	Wounding/Inflicting GBH Burglary and Theft - Non Dwelling Sexual Assault - Intentionally Touch Female - No Penetration AOABH Causing GBH W/I To Do GBH AOABH
13	07/03/2016	Robbery	Y	19/08/2015	Burglary and Theft - Non Dwelling
21	07/03/2016	Sexual Assault of Male Child Under 13	N	Has come to notice for non QO and received a caution	
20	18/02/2016	Cause/Incite Boy Under 13 To Engage In Sexual Activity - No Penetration	N	Has come to notice for non QO and received a conviction	
43	03/02/2016	Sexual Assault - Intentionally Touch Female - No Penetration	N	N/A	N/A
20	28/06/2016	Wounding With Intent To Do GBH	N	Has come to notice for non QO and received a conviction	
54	16/12/2015	Exposure	N	N/A	Came to notice for non QO under same arrest as S.63G offence and received a conviction
74	24/02/2016	Rape - Female Over 16 Years	N	N/A	Already had previous convictions keeping on biometrics
22	26/04/2016	Sexual Activity Female Child Under 16 Offender 18 Or Over Penetrate Anus/Vagina/Mouth By Penis/Body Part Cause/Incite Female Child Under 16 Engage Sexual Act Offender 18+ Penetrate Anus/Vagina/Mouth By Penis/Body Part	Y	16/01/2016 04/01/2016	Sexual Activity Female Child Under 16 Offender 18 Or Over Pentrate Anus/Vagina/Mouth By Penis/Body Part - NFA 1) Sexual Activity Female Child Under 16 Offender 18 Or Over Pentrate Anus/Vagina/Mouth By Penis/Body Part - Guilty 2) Sexual Activity Female Child Under 16 Offender 18 Or Over Pentrate Anus/Vagina/Mouth By Penis/Body Part - Guilty
17	22/03/2016	Rape of Female Aged 16 Years Or Over	Y	27/07/2016 20/11/2015	Rape of Female Aged 16 Years Or Over Causing GBH W/I To Do GBH
16	03/06/2016	Rape of Female Agred 16 Years Or Over	Y	17/03/2016	Wounding With Intent To Do GBH
38	02/02/2017	AOABH	N	Has come to notice for non QO and received a caution	
19	18/04/2016	Sexual Assault - Intentionally Touch Female - No Penetration	N	N/A	N/A
50	04/07/2016	AOABH	N	N/A	N/A
26	24/10/2016	AOABH	Y	30/09/2018	Assault/Ill-Treat/Neglect/Abandon A Child/Young Person To Cause Unnecessary Suffering/Injury
37	29/12/2016	Rape Of Female Aged 16 Years Or Over	N	N/A	N/A
14	09/02/2017	At/Rape of Female Aged 16 Years Or Over	Y	23/11/2018 14/06/2017	AOABH Robbery
12	27/04/2017	Cause/Incite A Girl Under 13 To Engage In Sexual Activity - Penetration	N	N/A	N/A
64	25/07/2017	Rape A Girl Under 13	N	N/A	N/A
34	15/12/2017	Rape of Female Aged 16 Years Or Over	N	N/A	N/A
15	18/08/2017	Robbery	Y	09/07/2018 29/04/2017	Robbery Robbery
25	02/11/2017	AOABH	N	N/A	N/A
45	18/10/2017	Possessing An Indecent Photograph Or Pseduo-Photograph Of A Child	N	N/A	N/A
35	18/09/2018	C/Rape of Female Aged 16 Years Or Over	N	N/A	N/A

Annex I – DNA matches

Match confirmed	Alleged offence(s)	Alleged offence subject of s.63G	On PNC	Current biometric retention status
Subject One	1) Robbery (Volume)	Robbery	N	Indefinite
	2) Using/Trading in/Shortening/Converting Firearms			
Subject Two	1) Abduction and Kidnapping	Wounding W/I To Do GBH	N	Indefinite
Subject Three	1) Less Serious Assault	Assault Occasioning Actual Bodily Harm	Maybe	Indefinite
	2) Wounding / Grievous Bodily Harm		Maybe	
	3) Robbery (Volume)		Maybe	
Subject Four	1) Robbery (Volume)	Assault Occasioning Actual Bodily Harm	N	Indefinite
Subject Five	1) Less Serious Assault	Wounding W/I to Do GBH	Maybe	Indefinite
	2) Other (Volume)		N	
	3) Attempted Murder		N	
Subject Six	1) Theft of a Motor Vehicle	Rape of Female Aged 16 Years Or Over	N	Indefinite
	2) Theft of a Motor Vehicle		N	
Subject Seven	1) Wounding / Grievous Bodily Harm	Causing GBH With Intent To Do GBH	Maybe	Indefinite
Subject Eight	1) Less Serious Assault	Sexual Assault - Intentionally Touch Female - No Penetration	Maybe	Indefinite
Subject Nine	1) Aggravated Burglary	Rape of a Boy Under 13	N	Held due to Live UZ Marker
Subject Ten	1) Burglary (Residential)	Burglary and Theft - Dwelling	Maybe	Indefinite
Subject Eleven	1) Burglary (Residential)	Assault Occasioning Actual Bodily Harm	Maybe	Indefinite
	2) Theft of Motor Vehicle		Maybe	
Subject Twelve	1) Rape	Sexual Assault - Intentionally Touch Female - No Penetration	No	Indefinite
Subject Thirteen	1) Robbery (Volume)	Robbery	No	Held due to Live UZ Marker
Subject Fourteen	1) Criminal Damage	Arson	No	Held due to Live UZ Marker
Subject Fifteen	1) Theft of a Motor Vehicle	Robbery	No	Held due to Live UZ Marker
Subject Sixteen	1) Burglary (Residential)	Causing GBH With Intent To Do GBH	No	Indefinite
Subject Seventeen	1) Wounding / Grievous Bodily Harm	Robbery	No	Held due to Live UZ Marker

LIST OF ACRONYMS

ABH	Actual Bodily Harm
ACPO	Association of Chief Police Officers (replaced by 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
CTBS Act	Counter-Terrorism and Border Security Act 2019
CTFS	Counter Terrorism Forensic Services (now known as Secure Operations – Forensic Services)
EAW	European Arrest Warrant
ECtHR	European Court of Human Rights
EMSOU-FS	East Midlands Special Operations Unit – Forensic Services
FINDS	Forensic Information Databases Service
FINDS-DNA	Forensic Information Databases Service's DNA Unit
FIND-SB	Forensic Information National Databases Strategy Board
FOI request	A request under the Freedom of Information Act 2000
FSPs	Forensic Service Providers
GBH	Grievous Bodily Harm
GDS	Government Digital Service
GMP	Greater Manchester Police
HMIC	Her Majesty's Inspectorate of Constabulary (England and Wales)
HMICS	Her Majesty's Inspectorate of Constabulary in Scotland
HMPO	Her Majesty's Passport Office
HOB	Home Office Biometrics Programme
IABS	Immigration and Asylum Biometric System
IDENT1	The national police fingerprint database
JCHR	Joint Committee on Human Rights
JFIT	Joint Forensic Intelligence Team
JSIU	Joint Scientific Investigation Unit
MOU	Memorandum of Understanding
MPS	Metropolitan Police Service
NCA	National Crime Agency
NCB	National Crime Bureau in the NCA

NDAS	National Data Analytics Solutions programme
NDNAD	National DNA Database
NFA	No Further Action
NLEDS	National Law Enforcement Data Programme
NPCC	National Police Chiefs' Council (which replaced 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

CCS0319869991
978-1-5286-1551-8