Annual Report 2019

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Paul Wiles

March 2020

Office of the Biometrics Commissioner

ANNUAL REPORT 2019

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.

July 2020

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 978-1-5286-2028-4
CCS0220195130 07/20

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. Priti Patel, MP
Secretary of State for the Home Department
Home Office
2 Marsham Street
London

19th March 2020

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 2019 which provides the above information. This is my first Report to you as Home Secretary but the sixth of the Commissioner for the Retention and Use of Biometric Material.

The main points in my Report are:

1. Compliance across law enforcement agencies with the requirements of the Protection of Freedoms Act is generally good with a high level of commitment from all law enforcement agencies.
2. Two recent Home Office changes have had significant consequences for the policing use of biometrics:

    i The changes to police bail introduced by the Policing and Crime Act 2017. I drew attention to the problems that the Act had created in my last two Reports and I welcome the review that you have announced.

    ii Codes guiding the police on the use of arrest powers and the subsequent growth of voluntary attendance rather than arrest have produced problems detailed in my last two Reports. The effect has been to reduce the number of initial speculative searches and of new DNA profiles and fingerprints added to the national databases. Unless this situation changes the usefulness of present and future biometrics to policing will decline and bring the overall investment in this technology into question.

3. The number of properly conducted policing trials of new biometrics and AI-driven analytics needs to increase in order to provide the evidence base that will be needed to make future decisions about the best new technology for policing. A standard trials methodology is needed.
4. Exploration by the police of the new biometric technologies and AI-driven analytics has been unnecessarily dampened by the failure of the Home Office to provide governance, leadership and re-assurance to support such work.
5. New legislation will be needed to bring these new technologies into a governance framework, and I welcome your Manifesto commitment on this matter.
6. Given the importance of these new technologies more generally in public and private sectors the public needs to be more engaged in a debate about what they regard as acceptable uses. Ministerial leadership would be welcomed on this.
7. The biometric provisions of the Counter-Terrorism and Border Security Act 2019 that are due to come into force shortly I believe will improve the consistency of decision making in relation to National Security Determinations.

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

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

FOREWORD

This report was completed and submitted to the Home Secretary on 19th March 2020. It is my last annual report as Commissioner since my term of office comes to an end in June. By then I will have been Commissioner for four years and throughout that time I have been supported by excellent civil servants.

I have had two Heads of Office. First Gemma Gyles and now Lucy Bradshaw-Murrow. Their job has not been straightforward. Since my appointment is part-time, they have had to speak on a daily basis for the Commissioner. To do so for an independent Commissioner is not an easy task when, as civil servants, their management is by and ultimately their loyalty is to the Home Office and the Home Secretary. They both managed this task with quite extraordinary professionalism whilst maintaining cordial relations with all the agencies that I was required to report on. Lucy is leaving my Office in April on a well-deserved promotion and she will be sorely missed for my remaining time as Commissioner. I sometimes hear criticisms of civil servants, but my experience has been of high quality work and advice combined with a professional integrity not often found in other areas. The Civil Service should be proud of them both.

The rest of my current team have been equally professional. Tahmida Hussain has been an excellent deputy head of office, Jalal Ahmed and Kamran Ali have ably supported me in deciding upon s.63 applications and Sahar Ajorloo has supported our complex arrangements for visits to law enforcement agencies and attendance at meetings and committees.

The Commissioner tends to get the public attention but in fact the work has always been a team effort and my thanks go to them all.

I understand that my job is not going to be replaced in June. At any rate there has been no advertisement for the public appointment of a new Biometrics Commissioner. I believe the intention is to make a joint appointment of one person as Biometrics Commissioner and Surveillance Camera Commissioner. Both these positions were created by the Protection of Freedoms Act 2012 although as separate roles. Whoever is appointed will have a huge task covering the previous workload of two Commissioners and covering two very distinct functions. I wish them well and hope that they find the role as rewarding as I have mine.

Paul Wiles
March 2020

CONTENTS

FOREWORD III

1. INTRODUCTION 1

2. FAILURES OF GOVERNANCE AND FUTURE GOVERNANCE NEEDS 3

3. BIOMETRICS FOR LAW ENFORCEMENT IN ENGLAND AND WALES 20

4. BIOMETRICS AND NATIONAL SECURITY 56

5. INTERNATIONAL EXCHANGES OF BIOMETRIC MATERIAL 71

APPENDIX A 83

APPENDIX B 87

APPENDIX C 91

LIST OF ACRONYMS 98

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 (PoFA) to provide assurance to the Home Secretary and to Parliament on the working of that legislation.

2. In the UK, responsibility for policing and crime investigation is devolved in the case of Scotland and Northern Ireland and so my remit only covers England and Wales. Scotland has its own legislation governing the use of biometrics by Police Scotland and has further legislation that has just been passed by the Scottish Parliament to extend and modify the governance of the police use of biometrics to cover new biometrics.[1] The Assembly in Northern Ireland passed similar legislation to PoFA, which included the creation of a Northern Ireland Biometrics Commissioner, but that legislation has still to be commenced.[2]

3. National security, however, is not devolved and my remit as regards the police use of biometrics for national security purposes covers the whole of the UK.

4. I am required to produce an annual report for the Home Secretary, and she in turn is required to lay that report before Parliament.

5. Beyond that I have two quasi-judicial functions in relation to police retention of DNA and fingerprints. These are:

   - Where there is no other power to retain a person's biometrics, but a Chief Officer of police decides that for reasons of national security they should be retained he/she can do so by making a 'National Security Determination'. I am required to examine all such Determinations and if they do not meet the legal tests required can order the destruction of the biometrics.[3]
   - Where the police in England and Wales have arrested but neither charged nor convicted a person, they cannot generally keep the biometrics that they took from the person on arrest. However, for certain more serious offences, the police can make an application to me to nevertheless do so on specific prescribed grounds.[4]

6. I am often referred to as a 'regulator' but I am not and have no regulatory powers. Instead the most important aspect of my role is to provide the independent oversight that Parliament thought necessary in giving the police considerable powers to take, retain and use biometrics. Strictly speaking my role is quite limited but I, like the first Commissioner, have felt it right that I should report to the Home Secretary on the growth of new biometrics and policing interest in them.

7. This is the sixth Annual Report of the Biometrics Commissioner and my final one as Commissioner.

1 For further discussion of this see Chapter 2.
2 http://www.legislation.gov.uk/nia/2013/7/schedule/2
3 See Chapter 4 of this Report.
4 See Chapter 3 of this Report.

8. 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. That judgment 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.[5]

9. The new proportionality put in place by PoFA is, like all legislation, itself open to further challenge in the courts. We have had such challenges to the police retention of custody images,[6] to the use by South Wales Police of Live Facial Recognition (LFR)[7] and to the indefinite retention by the Police Service of Northern Ireland (PSNI) of DNA profiles, fingerprints and custody images from convicted persons[8]. The implications of these judgments will be discussed later in this report.

10. 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 quality of other biometric technologies. Digital facial images are now routinely collected and stored by the police and the Metropolitan Police Service have started the operational use of live facial image matching in public places. Other technologies, such as voice recognition and gait analysis, are also being trialed 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. This issue is discussed further in Chapter 2 of this Report.

11. 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 she considers would be contrary to the public interest or prejudicial to national security.[9] No such exclusions have been made by any Home Secretary to any previous report and it is my hope that this Report will also be published in full.

5 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.

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

7 *R (Bridges) v CCSWP and SSHD* [2019] EWHC 2341 (Admin)

8 *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.

9 PoFA section 21(5)

2. FAILURES OF GOVERNANCE AND FUTURE GOVERNANCE NEEDS

INTRODUCTION

12. Since becoming Commissioner almost four years ago I have explained why the emergence of new biometrics, that could have a policing use, are not adequately covered by the current governance arrangements, and that new governance is necessary to allow the police to conduct trials and certainly if they routinely deploy new biometrics. I have also argued, as did my predecessor, that new legislation would in the end be necessary to create those governance arrangements. For most of my time in office it has been clear that making this case has not been welcomed by government. However, the manifesto of the new government elected in December 2019 proposed such new legislation, which I welcome.

13. I have regular contact with the police which includes discussing their current and possible future use of biometrics and I am in a position to observe at first hand how current governance has worked and whether new governance would be helpful. However, as a Commissioner I am a publicly appointed office holder. As such I do not have the legitimate mandate to propose the content of new legislation or how new governance should be provided: that is for Ministers in the first instance and then for Parliament. My position is constrained by my role under the Protection of Freedoms Act and it is proper that it should be so. For that reason, whilst I have explained why my advice is that new legislation governing (at least) the police use of new biometrics should be developed, and, identified some of the issues that need to be considered, I have not said what the content or form of that legislation should be.

ROLE OF THE BIOMETRICS COMMISSIONER

14. The job of the Biometrics Commissioner, apart from the two areas of casework discussed in subsequent chapters, is to report to the Home Secretary and thence to Parliament on compliance with the governance put in place by the Protection of Freedoms Act 2012 (PoFA) and more generally on the governance of the police use of biometrics[10]. Biometrics are an especially sensitive source of data because they are specific and personal, and often can be used to reveal other sensitive information about the individual. This has generally been recognised by legislators: for example, our latest data protection legislation draws attention to the sensitivity of biometric data[11]. PoFA also recognised this sensitivity by making rules as to when the police can take and retain biometrics and what they can be used for but also by providing an independent element in the decision-making process and independent oversight of compliance by creating the role of Biometrics Commissioner. It should be noted that I am not a regulator: I have no enforcement powers since my role is to report to the Home Secretary.

15. Since PoFA came into force in 2013, problems with compliance have gone through three phrases:

    1. questions about the meaning and interpretation of PoFA;
    2. the consequences for biometric use by the police of changes made by the Home Office for other reasons and;

10 I refer here to 'police' but PoFA in fact applies to a range of law enforcement agencies listed so the reader should bear in mind the wider application.

11 Data Protection Act 2018, Part 3, s. 35(8)(b)

3. police experimentation with new biometrics and the introduction of new databases.

16. These governance issues have mainly arisen under the sections of PoFA that apply to England and Wales because routine policing governance is devolved to Scotland and Northern Ireland. There are governance issues that apply to the use of biometrics by the police for national security purposes but since this is not devolved then they apply to the UK and are discussed in Chapter 4 on national security biometrics.

INTERPRETING POFA

17. The first phase of governance issues started immediately after the legislation came into force and was essentially about how the legislation applied or concerned police forces unsure how to comply with the legislation.

18. My predecessor, Alastair MacGregor QC, dealt with many of these questions by providing advice on straightforward matters and most of these issues were dealt with quickly. Where he did not think that it was appropriate for him to give advice, he suggested that the police take independent legal advice. Again, most of these cases were dealt with fairly quickly.

19. Where neither of these responses was appropriate, he suggested that the Home Office should provide guidance for the police. However, this resulted in a dispute over who should issue any such guidance since the police regarded it as the Home Office's role to provide guidance on their legislation, but the Home Office regarded it as the role of the police to provide post-legislative guidance. However, by various routes much of the required guidance has now been issued, although some remains outstanding despite promises made in the Ministerial responses to previous Reports.

20. The type of issues raised in this first phase are not unusual after the passing of new legislation but have been more visible in this case because of my Office's role in raising them and reporting on them in an annual report. It does raise the interesting question of how well such issues are dealt with for other new legislation where there is not independent oversight.

21. The result of this first phase is that there is now a well understood process of governance for the police use of DNA and fingerprints that is workable and compliance is now generally good. The occasional exception to this picture is usually due to a change of the responsible police leadership either without adequate handover or the new leadership simply starting again.[12]

CONSEQUENCES OF OTHER HOME OFFICE ACTIONS

22. The second phase of compliance issues arose as the unintended consequences of other action taken by the Home Office, either by way of guidance or new legislation that raised new problems for the police use of biometrics. The most important of these are the increasing use by the police of interviewing suspects on a voluntary basis as a result of a new code of practice[13] on the use of arrest powers and the restriction on the use of bail as a result of the Policing and Crime Act 2017.

12 This a more general problem in policing. See K. Pease and J. Roach: *How to morph experience into evidence* in J. Knuttson and L. Thompson (eds): Abingdon, Routledge, 2017.

13 PACE 1984 sets out the core powers of the police to prevent, detect and investigate crime. The exercise of these powers is, however, subject to codes of practice, or PACE codes, which the Secretary of State is required to issue under sections 60, 60A and 66 of PACE. The PACE codes do not create new powers but give guidance as to how the police should exercise those powers. Code G of PACE, which relates to the use of the power of arrest, was revised in 2012.

23. I have questioned in my previous Reports how far the Home Office should have foreseen the problems that these changes created. These issues are reported on further in the next chapter and the Home Secretary has announced a review of the bail changes. There remains the risk that further changes in policing could again have unintended consequences for the use of biometrics.

POLICE INTEREST IN NEW BIOMETRICS

24. The third phase of compliance issues has emerged because the police are experimenting with new biometrics that are not covered by the governance arrangements created by PoFA and by the Home Office developing new databases to hold the police and other agency's biometric data on shared data platforms. These will be discussed further below since they have raised significant media attention, critical comment, legal action and an investigation by the Information Commissioner. The present concerns have focused on the police experimenting with facial recognition technology, but this is just the first of the new biometrics that the police are considering for operational use.

HISTORY OF BIOMETRIC USE BY THE POLICE IN ENGLAND AND WALES

25. The use of biometrics by the police in the UK is almost as old as modern policing itself, having its origin in the late nineteenth century and involving the police taking fingerprints and photographs. However, this early use of biometrics was limited since searching for matches involved making comparisons with paper-based reference collections, which was slow, constrained by the need to keep reference collections manageable in size and therefore limited usually to local collections.

26. A hundred years later, the growth of computing and the realisation that DNA could be used for forensic purposes led to a technical revolution. DNA profiles can be derived from DNA samples and since they are expressed digitally can be stored on a computer database. This removed many of the previous limitations on the police use of biometrics because machine digital matching became possible and the reference collection being searched could be national, or even international. DNA was the first true modern police 'biometric' and a national DNA database was set up in 1995 by the Home Office, the first of its kind anywhere. Fingerprints later followed and local paper collections were replaced by a national fingerprint database. Digitally matching photographs proved more difficult and had to wait for the next generation of technical changes.

27. A further technical revolution is happening now and is driven by our ability to build ever larger databases and then to use artificial intelligence (AI) on those databases to develop algorithms for biometric matching. This development of AI-driven analytics, however, is speeding up the development of a wide range of new technologies and will affect all areas of our future life. As far as the police use of biometrics is concerned the first visible result is the new ability to use digital facial images in a similar way to DNA and fingerprints; in other words, those old mugshots have become modern digital biometrics. The growth of the new AI-driven technologies has been very rapid and has meant that over the last five years facial matching algorithms have improved exponentially. However, facial matching is just the first of a range of new biometrics that are becoming available and could be used by the police.

GOVERNANCE OF BIOMETRIC USE BY THE POLICE

28. The historical development of biometric use by the police in England and Wales slowly came under legislative control. The first significant governance was introduced by the Police and Criminal Evidence Act 1984 (PACE), which required police to destroy fingerprints and DNA samples that were taken during a criminal investigation if an individual was not convicted of an offence.[14] From 2001 the police were allowed to keep biometrics indefinitely if an individual was charged but not convicted of an offence and from 2003[15] to do so even if an arrested individual was neither charged nor convicted. However, in 2008, the European Court of Human Rights held in response to a challenge to this position that England and Wales and Northern Ireland were the only Council of Europe members who allowed such indiscriminate retention of DNA and fingerprints and because this failed to strike a fair balance between public and private interests it was not proportionate.[16] In response the Labour government passed the Crime and Security Act 2010 which reduced some retention periods but before the Act was implemented a general election intervened.

29. The incoming coalition government repealed that Act and instead introduced the Protection of Freedoms Act (PoFA) in 2012, which generally restricts the indefinite retention of DNA and fingerprints to those convicted of a recordable offence but allows some retention for those charged but not convicted and limited retention for those arrested for more serious offences but not charged on application to the Biometrics Commissioner. The Act also allows for retention of biometrics on the grounds of national security by the granting of a National Security Determination by a Chief Officer of Police. Finally, PoFA allows the police to keep the DNA profile but not the DNA sample to guard against the DNA material been used for any other purpose than that authorised.

30. The present situation, therefore, is that we have legislation governing the police use of DNA and fingerprints which was passed in response to a judgment of the European Court of Human Rights. However, we have just had a further judgment from the same Court in the case of Gaughran.[17] The Gaughran judgment again raises questions about the proportionality of the current governance of the police use of biometrics and points to the lack of adequate review of police retention of biometrics. In particular, the Court found that '*the indiscriminate nature of the powers of retention of the DNA profile, fingerprints and photograph of …[a] person convicted of an offence, even if spent, without reference to the seriousness of the offence or the need for indefinite retention and in the absence of any real possibility of review, failed to strike a fair balance between competing public and private interests.'*[18] The judgment also goes beyond PoFA governance, since it covers the police use of facial custody images as well as DNA and fingerprints. Interestingly the court also drew attention to how the growth of the new biometrics requires a re-examination of governance.

31. Furthermore, as just explained the usefulness of the new biometrics is being driven by the use of AI analytics which are also being explored more generally to see how far they could have other uses for policing. The Home Office has funded a trial with West Midlands Police to examine whether such analytics could be used to predict future offending[19] and other forces

14 PACE 1984 sections 61-63.
15 Criminal Justice and Police Act 2001 and Criminal Justice Act 2003
16 *S and Marper v United Kingdom* [2008] ECHR 1581
17 *Gaughran v. the United Kingdom* [2020] ECHR 060
18 Ibid, para 96.
19 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812351/Biometrics_Commissioner_AR_2018_Print.pdf para. 47

are also exploring other uses. Biometrics then are just one data source that can be explored by AI driven analytics for possible police use.

LIMITATIONS OF CURRENT GOVERNANCE

32. The police use of fingerprints and DNA is now mature and the governance of their use has evolved over time as a result of both technical developments and legal challenges that have led to a series of legislative changes. That process continues but the specific legislative control of the police use of biometrics in PoFA applies only to fingerprints and DNA; that is the governance arrangements laid down in PoFA do not apply to the new biometrics that the police are now interested in exploring.

33. Deployment by the police of any of the new biometrics will raise all the same governance issues as do the police use of DNA and fingerprints: namely the rules for the police acquisition, retention, use and destruction of biometric material. In addition, the Home Office's development of multi-user data platforms raises the question of whether there should also be governance of data sharing. This in turn raises the question of whether any police deployment of new biometrics should be governed by legislation in the same way as DNA and fingerprints either by an extension of PoFA governance, or by similar new legislation putting in place governance for the new biometrics, or by new legislation replacing PoFA and providing governance of all future police use of biometrics?

THE GROWTH OF PUBLIC CONCERN

34. Initially, concern about the police use of new biometrics was limited to specialist civil liberties groups. Indeed, when I met the Home Office Minister responsible for biometrics, just after my appointment, and raised the issue of further governance she understandably pointed to the lack of evidence of wider public concern and when I suggested that might be about to change my evidence was limited and rather technical. However, change it has for a number of reasons.

35. The emergence of global tech companies meant that they acquired very large data sets of personal information about their users. The new analytics and especially the development of AI meant that those holding large amounts of data can use the data to develop new understandings of people's behaviour and how that behaviour might be predicted or influenced. Initially the tech companies found it difficult to combine their desire to allow free public access to their platforms with their long-term need to make a profit. Advertising on the platforms provided some income but it was the realisation that selling the analysis of their data could provide significant income that changed their profitability. This business model has made the global tech companies very wealthy but depends on using the personal data they hold in ways which their users often are not aware. This was laid bare as a result of media investigations, American political hearings and because of a very detailed academic study that argued that this was a new form of business that depended on public surveillance.[20] This was followed by the realisation that tech company's platforms were also being used by third parties to collect data for other reasons, most controversially for political purposes.[21]

20 See: Shoshana Zuboff: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, London: Profilebooks, 2019

21 In the case of the UK especially the reporting by Carole Cadwalladr in the Guardian of the work of Cambridge Analytica.

36. Public awareness has grown of how AI-driven data analytics enables the monitoring and understanding of our behaviour, motivation and thinking across a wide range of our life and the possibility of predicting or altering our action. Some of the claims being made for such capabilities by the developers of new algorithms may be a little ahead of the evidence but not against the direction of the technical changes that are happening.[22] At any rate many countries are exploring the possible use of such systems. In England and Wales, the police are interested in exploring both new biometrics and data analytics and the Home Office is funding trials in both areas.

37. What especially galvanised public concern about the use of these new technologies, however, was the trials carried out by the police of the use of live facial recognition systems (LFR) in public places. This was almost bound to be the case because unlike existing police biometrics whose acquisition is quite complicated, digital facial image capture is easy and the subject may not even be aware that it has happened.[23] For the same reason, faces in public places can be easily scanned and matched. In other words, this is potentially much more intrusive of an individual's privacy than existing police biometric use. That is not to say that there may not be a public interest case that justifies such intrusion when balanced against the public benefits derived. However, the trials inevitably raised the question of whether the police use of LFR in public places was so justified?

THE CHALLENGE TO POLICE USE OF LFR

38. There was significant reaction to the police use of LFR. There were both media and political requests for greater transparency, civil liberties groups questioned whether uses of LFR in public places by the police could be justified as in the public interest and a similar debate in the US led to some cities banning the use of facial matching by their police forces. In this country *Big Brother Watch* published an open letter demanding a halt to the police use of LFR which was signed by a number of leading politicians.[24]

39. A legal challenge was made by *Liberty*, against South Wales Police, and *Big Brother Watch* who currently have a stayed challenge against the Metropolitan Police Service.

40. In the South Wales Police case, the Court decided that their use of LFR was consistent with the requirements of the Human Rights Act and data protection legislation and lawful in pursuit of the Police's common law power to prevent crime and arrest offenders. It also found that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of the LFR as it was used in trials by South Wales Police.[25]

41. The judgment considered solely the use of LFR by the police and not by any other public or indeed private body. It should also be noted that this is a judgment in the first instance and that the claimant has appealed. This is not surprising given the fundamental rights at stake and that, as is stated in the judgment, this is the first time that any court in the world has considered LFR.

22 For example, there is concern as to how far the theory behind the use of facial imaging to read emotions is reliable. See: Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements. Psychological Science in the Public Interest, 20, 1–68

23 Facial capture is sometimes referred to as 'frictionless' compared with DNA or fingerprints.

24 The leader of an opposition party, the shadow Home Secretary and the Chair of the Common's Science and Technology Committee.

25 *R (Bridges) v CCSWP and SSHD*, [2019] EWHC 2341 (Admin)

42. It is not for me, as Commissioner, to comment on the High Court's judgment or the likely outcome of an appeal. For the present the police have a lawful basis for using LFR but are aware that the Court stressed that its judgment related to the specific way in which South Wales Police had conducted their LFR trial.

43. The bigger question going forward is whether there should be new legislation that provides new rules for the police (and perhaps others) use of new biometrics, including LFR but also voice recognition, gait analysis, iris analysis or any other new biometric technologies as they emerge. The alternative is that we are likely to see further legal challenges to other biometric use by the police. In the absence of new legislation such challenges will be helpful in clarifying how the police may act but will mean that the police exploration of new biometrics will be slowed and rely on judge-made law, something that most of the judiciary do not like doing, preferring that if there needs to be a legal responses to social and technological change that it should be through legislation made by Parliament.[26]

CONTINUING POLICE INTEREST IN NEW BIOMETRICS

44. The South Wales judgment was greeted by the government as justifying their belief that there was a legal basis for the police use of LFR and therefore there was no need for new legislation to regulate the police use of new biometrics.[27] However, what the government had done prior to the judgment was to set up a Governance and Oversight Board to create a framework for the police use of new biometrics[28] and the existence of that body was one of the things that the Court pointed to in deciding that the South Wales Police's use of LFR met the general tests for legality.[29] I together with the Surveillance Camera Commissioner and Forensic Science Regulator agreed to sit on the Board to help create a pre-legislative governance framework for the police use of new biometrics. In fact the Board made no progress in developing such a framework nor provided significant oversight.[30] That is unfortunate since it has meant that the Board has not done any pre-legislative thinking and without such a signal from government then much of the senior leadership in policing, as well as the Police and Crime Commissioners (PCCs), are reluctant to explore uses of the new biometrics and AI-driven data analytics for policing purposes. The South Wales judgment has confirmed a legal basis for the use of AFR but the failure to provide proper governance or guidance to the police is impeding technical development in policing.

45. If the police are going to examine possible uses of new biometrics then it is important that they are able to conduct trials before considering deployment. This is so that the utility of new biometrics can be systematically examined together with the human decision making and operational concepts that will be needed alongside the biometric use. It is equally important that such trials meet proper scientific standards and preferably include an independent element in their evaluation: in other words they meet the kind of trials methodology that are common in other areas of public policy.[31] Conducting trials must be done with an open mind and not simply as a precursor to an already decided deployment: an aspect of standard trials

26 For a statement of this position see: Sumption, J: Trials of State: Law and the Decline of Politics, London, Profile Books, 2019.
27 https://hansard.parliament.uk/Lords/2019-10-02/debates/98E04E57-E587-4F2E-900D-9082450AFB90/FacialRecognitionTechnology?highlight=live%20facial%20recognition#contribution-7BAFC326-B6C0-423F-9C59-7ACD3A52EDE8
28 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784855/Facial_Images_Board_TOR_Final_Version.pdf
29 *R (Bridges) v CCSWP and SSHD* [2019] EWHC 2341 (Admin), paragraphs 9 and 44.
30 A point also made by Dr Gillian Tully, the Forensic Science Regulator https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868052/20200225_FSR_Annual_Report_2019_Final.pdf pp. 23-24.
31 The need for such a methodology was discussed by the Law Enforcement New Biometric Modalities Oversight and Advisory Board but not acted on.

methodology is that what is to be evaluated, and how it will be evaluated, is made public in a published protocol before a trial begins to ensure the purpose is clear and doesn't shift according to the findings of the trial.

46. This rigour matters because at some point in the future the police will have to decide which of the large number of biometrics that are becoming available are optimal in achieving the public purposes of policing. Without proper trials being conducted they will not have the evidence to make such a decision, nor will they know the cost benefits of deploying a particular mix of biometrics. Nor will a proper understanding be developed of how new biometrics may be used in the criminal justice process and especially in evidence[32]. I welcome the fact that the latest trials being run by the Home Office are using such rigour in their design and evaluation.

OTHER RESPONSES TO CONCERNS ABOUT LFR

47. Other bodies outside of government have been discussing whether there ought to be legislation to govern the use of new biometrics. The work of the civil liberties groups in the UK in challenging the police's use of new biometrics has already been mentioned. In addition, there are a number of both national and international groups who have been discussing the issue.

48. In the UK the government's Centre for Data Ethics and Innovation (CDEI) exists to connect policymakers, industry, civil society, and the public to develop the right governance regime for data-driven technologies. It commissioned a report by the Royal United Services Institute (RUSI) into bias in the algorithms developed for policing [33] and plans further work on data driven systems in policing. The Centre's mission is to ensure that governance arrangements are in place that allow and not prevent the exploration of new data driven technologies in a controlled way rather than preventing them entirely.

49. Both the South Wales Police and the Metropolitan Police's use of LFR have been independently evaluated by university researchers.[34] The Mayor of London's police ethics group has also published a report on the use of LFR[35] as has the Home Office Ethics Group.[36] The Nuffield Foundation published a report on *'Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research'*[37] Nuffield has helped fund the Ada Lovelace Institute[38] which is exploring public expectations and legal regulation of biometric data and related technologies, in particular looking at facial recognition. During 2020 they are setting up a 'Citizens' Biometrics Council' to look at the social and ethical factors engaged by biometric technologies. They are also carrying out an Independent Review of the Governance of Biometric Data. This work is particularly interesting because the changes that biometrics may make to policing need to be based on a good understanding of the public(s) attitudes to the various use cases of new biometrics that the police may be interested in. To fail to have good

32 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868052/20200225_FSR_Annual_Report_2019_Final.pdf p. 22
33 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf
34 See: http://afr.south-wales.police.uk/cms-assets/resources/uploads/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf and https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf
35 http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf
36 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf
37 https://www.nuffieldfoundation.org/wp-content/uploads/2019/12/Ethical-and-Societal-Implications-of-Data-and-AI-report-Nuffield-Foundat.pdf
38 The Ada Lovelace Institute was established in 2018 by the Nuffield Foundation in partnership with the Alan Turing Institute, the Royal Society, the British Academy, the Royal Statistical Society, the Wellcome Trust, the Omidyar Network for Citizens and Governance, techUK and the Nuffield Council on Bioethics.

quality information on public attitudes or fail to take it into account would risk damaging trust between policing and the public on which our model of policing is based. A number of other bodies have held or are planning to hold events to discuss either the police use of LFR or the broader questions around the use of new biometrics or AI.

50. In many other countries and internationally there is a similar interest in exploring the implications of new biometrics, often together with AI. The Biometrics Institute is an international organisation that has worked with the biometrics industry but also the United Nations and national bodies to develop standards for implementation and privacy for the use of biometrics.[39] It is interesting that many of its industry members are now in support of regulation of biometric use, including some of the major players such as Microsoft.

LEGISLATION GOVERNING THE USE OF BIOMETRICS IN THE UK – DATA PROTECTION

51. In addition to a common law power justifying the police use of LFR, there is legislation providing governance of the police use of biometric data, namely the Data Protection Act 2018.

52. The Data Protection Act brought into UK law the requirements of EU regulation of the use of personal data as set out in principle in the General Data Protection Regulation (GDPR) and includes special provisions for the processing of data by law enforcement.[40] The Act is enforced by the Information Commissioner and she has already examined the use of LFR by the police,[41] has commented on the South Wales Police judgment,[42] and is investigating the use of LFR by private bodies.[43] Unlike me the Information Commissioner is a regulator and has significant powers to ensure that any use of LFR abides by the requirements of data protection legislation and she has made clear that she is prepared to use those powers if it does not.

53. This raises the question of whether data protection legislation covers all the matters of principle that are thought necessary to govern future police use of biometrics.

54. Data protection legislation, as already explained is based on the GDPR principles that are essentially designed to protect people's privacy since privacy is seen as a good in itself.[44] However, that value can easily conflict with other values, such as actions which deliver benefits to a collective or public interest. Tensions between different values involved in our behaviour are inevitable since very few actions simply relate to only one value. It is in the essence of social behaviour and especially the political consideration of social behaviour that such tensions have to be decided upon and then managed. That is why a central part of previous legislation governing the police use of biometrics is how that tension should be resolved: what is the balance between the individual's right to privacy and the public benefits that will derive from police use of DNA and fingerprints. It is what lawyers refer to as 'proportionality' and it has been central to the legal challenges that have been made to the governance of the police use of DNA, fingerprints and custody images.

39 See:https://www.biometricsinstitute.org/what-is-biometrics/standards/
40 See: https://ico.org.uk/for-organisations/guide-to-data-protection/
41 https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
42 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
43 See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/
44 At least that is so in the western thought tradition but not necessarily so in other traditions which place more emphasis on collectivism.

THE ROLE OF POLITICAL DECISION MAKING

55. If the question of proportionality is central to the governance of the police use of biometrics then it leaves the question of how that should be decided. That in turn has two aspects: namely who should decide and on what basis?

56. At present we have a mixed picture on who should decide on proportionality for the police use of biometrics. For DNA and fingerprints proportionality has been decided by Parliament and passed into statute. In the case of the new biometrics the decision is currently being made by the police. Some police leaders are unhappy with that position since they fear that taking the decision may not be seen as legitimate and therefore risk public trust in policing. The result is that many police forces are very cautious about using the new biometrics, especially LFR. This is understandable at a time when there has been a reported decline in trust in public institutions that has also been linked to a decline in confidence in democratic government.[45]

57. As things stand the Information Commissioner or court judgments may limit some possible uses by the police of LFR or other biometrics. But the South Wales judgment has already revealed some tension between these two routes.[46]

58. In the past, ultimately it has been for Parliament to decide what police use of biometrics is proportionate. That is because in a democracy balancing citizen's individual rights against whether any state interference in those rights is justified is a political matter to be decided by the body that has a legitimate power to make such decisions, namely Parliament. In the end it is for Parliament to decide whether we wish the police in England and Wales to use LFR or other new biometrics and if so for what purposes. The question now is how soon there should be new legislation that provides rules for the police (and perhaps others) use of new biometrics.

POSITION OF THE NEW GOVERNMENT

59. The previous government felt that legislation to govern the use of new biometrics by the police was unnecessary and welcomed the South Wales judgment as justifying that position.

60. However, the Conservative Party under its new leader, Boris Johnson, said in its recent manifesto:

> *"We will embrace new technologies and crack down on online crimes. We will create a new national cyber crime force and empower the police to safely use new technologies like biometrics and artificial intelligence, along with the use of DNA, within a strict legal framework. We will also create a world-class National Crime Laboratory."*

61. Manifestos are brief statements of intent and the intention did not feature in the recent Queen's speech, so I assume that this will not happen in this session of Parliament.

45 https://www.cambridge.org/core/journals/american-political-science-review/article/in-the-mood-for-democracy-democratic-support-as-thermostatic-opinion/D92BFDDD1565D610C38A0AA88DDBA102

46 See:https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

THE POLICE RESPONSE

62. Whilst police leaders are cautious about deploying the new biometrics without a clear governance framework, two forces have been less constrained. The South Wales Police, on the basis of the Cardiff High Court judgment, are continuing to trial LFR in public places, most recently at a local football derby. The Metropolitan Police Service (MPS) announced in January 2020 that they would proceed with operational deployment of LFR. This is a step change from trial to operational deployment. Before starting such deployment, the MPS placed on their website a legal mandate for their use of LFR and a guidance document for the governance of the deployment. These are designed to demonstrate the legality of their use of LFR and that they are staying within the jurisprudence of the South Wales judgment. This is a legal response but what will also matter is how far the public decide that what the MPS are doing is acceptable.[47]

63. Some of the new crime challenges which the police face spring from the same technologies that have opened up the possibility of new policing technologies. It is understandable that police leaders wish to explore those same technologies to respond to the problem which they are creating. Problems for policing have come not just from new biometrics but from broader technical change, such as the huge amounts of digital evidence, and the developing range of AI-driven data analytics that private companies are exploiting much more quickly than the police. At the same time public trust in policing must be retained as new technologies are deployed. The mere fact that private companies are using many of the same technologies does not mean that in using the same technologies the police can assume public trust. The police will always be a special case because they embody the power of the state to sanction behaviour deemed unacceptable. The common recent change of title from police force to police service doesn't elide this fact. We have developed a system of policing that justifies enforcement on the basis that decisions as to what behaviour to sanction are seen as legitimate. This legitimacy allows the police to govern by consent and enjoy public trust to do so. Trust is maintained by a delicate balance between the legitimacy of democratic law making by Parliament and the police acting within and being in turn governed by the rule of law. Like the judges, the police would prefer that government provided rules governing the use of new technologies rather than leaving it to the police service in order to protect the trust on which policing depends.

BIOMETRIC USE BEYOND POLICING

64. We are all aware that the new biometrics, such as facial matching, are being used more widely both elsewhere in the public sector, such as by local government and in the private sector, for example by shopping malls or residential buildings. The Home Office has no systematic record of such uses and has found itself reacting to examples revealed either by the media or civil liberties groups.

65. However, this growing use of biometrics by private organisations raises a number of issues. First, any use of biometrics will raise the same issues as use by the police but this is especially so when they are being used for a private policing purpose. Because the purpose is in pursuit of a private interest then any claim that the use is in the public interest will need more careful scrutiny when it is being done by those without a public mandate for policing to rely on. Secondly, many of the companies offering such technologies claim to fulfil a public

47 See: https://www.adalovelaceinstitute.org/changing-the-data-governance-ecosystem-through-narratives-practices-and-regulations/

interest and seek to demonstrate that by offering to share the data which they capture with the police.[48] In some circumstances such an offer may be acceptable but the fact that it is made with a clear commercial vested interest means that it needs to be challenged and judged independently. There is some interest within policing in accessing such privately held data, ranging from shopping mall facial images to DNA held by private companies in return for analysis of a customer's ancestry. As the range of such data expands there needs be a clear framework for deciding whether such sharing of data is in the public interest. Thirdly, and more generally, we are all now aware that the exploitation of our personal data for profit is built into the business models of those who routinely harvest our data whilst offering us services and products, from the global tech companies to the small online retailer. Indeed, some commentators have suggested that the main business even of large on-line retailers is actually data exploitation by trading in data. This wider use has also led to a range of legal challenges across Europe[49] but also by moves by the global tech companies to avoid GDPR regulation as Britain leaves the EU.[50]

66. The sharing of capabilities and data between the private sector and the police needs a governance framework but so also does the same sharing within the public sector. Government is a very large holder of personal data but so far datasets have been largely tied to a single function. Some limited data sharing has happened usually under a legislative mandate, for example between the police and immigration fingerprint databases.[51]

67. That position is changing because single-use government databases are being replaced by multi-user data platforms and big data software is now available that makes analysis across a number of databases practical. We have always known that government data holdings were analytically under-exploited and a great deal of added value could be released by analysing across databases. But the very fact that data sharing and cross-database analysis is now much more possible makes it necessary that we have a cross-government data sharing governance framework in place.

THE PROBLEMS

68. My reason for highlighting these issues is to illustrate how complicated creating a system of governance is going to be. We have allowed a new technology to develop rapidly across the fabric of our society without being clear about the implications and whether we wish to allow uncontrolled development. In part this is because of a fatalistic belief in technological determinism: that either technological development has an inevitability beyond government control or that any attempt at control will unnecessarily limit the innovation on which our future prosperity depends. This is a fallacy; AI is a product of human intelligence and ingenuity not some determinate force of either divine or historical inevitability. The same intelligence and ingenuity should decide how we want to use new technology. All previous examples of the kind of profound technical change that we are now experiencing have faced the same concerns before governments realised that technology can be steered by a vision of the future world we want to create and that well-made governance can actually support, rather than limit, innovation.

48 Or at least they used to. I note that many companies have now removed such statements.

49 For example, the Dutch Government's fraud algorithm SyRI breaks human rights, privacy law. See: https://www.dutchnews.nl/news/2020/02/governments-fraud-algorithm-syri-breaks-human-rights-privacy-law/ and in Sweden the data protection regulator has ruled against the use of facial recognition in schools. See:https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/

50 https://www.reuters.com/article/us-google-privacy-eu-exclusive/exclusive-google-users-in-uk-to-lose-eu-data-protection-sources-idUSKBN20D2M3

51 Although see Chapter 4, paragraphs 242 to 248 of this report for an example of data sharing that has happened without such a mandate.

69. In addition, as a country we are remarkably careless with our civil liberties. We have allowed the development of CCTV coverage on a scale second only to that in China and the public response to that and police use of facial matching has been muted. Other European countries have asked more searching questions and to them we owe the response of the GDPR, and in the USA serious questioning has happened at both at state and federal level. Why this should be so I suspect is because we are the European country which escaped the Second World War horrors linked to invasion and state repression and because, unlike even most other common law jurisdictions, we are not citizens that have learned the meaning of citizenship from a founding constitution.

70. Many of the uses of the new technologies are either benign or are likely to be judged in some sense as in the public interest. In other words, the intrusion into our individual privacy may be acceptable when set against the benefits we derive. However, some uses of new technology may equally not be in the public interest nor justified by the benefits that we derive. Neither Luddism nor allowing the private interests behind technology free reign are therefore sensible responses. That is why I want to conclude this chapter by discussing two issues. First, the complications of legislating to govern the impacts of the new technologies and secondly, why addressing this issue will mean making a strategic political choice.

LEGISLATING FOR NEW BIOMETRICS

71. The question of whether we should create a legislative framework for the new biometrics is not just being asked in England. The EU are asking the same question as are some States in the USA and to judge by the requests that I receive for interviews about the issue also many other countries. Leading the way in the development of legislation is, however, Scotland who already passed a Bill to govern the police use of new biometrics through the Scottish Parliament.[52]

72. Enacting such legislation is not easy and all countries are facing common problems. Logically, before turning to the form of future legislation, comes the question of whether these new technologies are worth deploying in policing. This is a question about:

    1. Does a biometric algorithm do what developers claim?
    2. Does the technology also work in real world policing situations in a robust manner?
    3. What are the identifiable limitations (such as bias) of an algorithm and can these be overcome in the subsequent decision making?
    4. Does a new biometric actually add value to existing non-biometric policing practice to justify its costs and risks?
    5. Have the police developed a concept of operations to go alongside any new biometric before it is deployed?
    6. If algorithms continue to 'learn' whilst in operational use is this transparent and can it be dealt with practically in policing, or does such learning in use need to be restricted?

73. All of these questions point to the importance of running trials of new biometric technologies before any operational deployment in policing.

52 https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx

74. When it comes to thinking about legislation there must firstly be thinking about the form of that new legislation, particularly:

    1. Can legislation be flexible enough to respond to the speed of technical change? Legislators who seek to deal simply with a current concern, such as the police use of LFR, will quickly find that they are firefighting the next problem. A way has to be found to legislate for current and future uses of biometrics.
    2. If legislation is to be flexible, then how and by whom will such flexibility be provided for as yet unknown future biometric uses?
    3. Then there is the question of scale: should we seek to legislate just for biometrics or more broadly for all AI-driven analytics?
    4. Then is the question of range: should legislation govern the police use of biometrics, or should it extend to all public sector use, or all use by anybody?

75. These questions need to be decided before moving onto the practical problems of framing legislation.

76. Second are questions of whose biometrics and on what basis we think the police should be able to take and retain:

    1. Should the police only be able to take biometrics if they arrest someone as at present?
    2. Other than legally sanctioned covert operations, should the police be allowed to capture biometrics other than on arrest? For example, facial image capture on the street without the subject's knowledge?
    3. When should the police be allowed to retain biometrics? As at present for DNA and fingerprints, of those convicted of a recordable offence? Should there be any additions to this general rule?
    4. For how long should the police be able to retain the biometrics which they are authorised to keep? At present it is 'indefinitely' but that has been criticised as not being proportionate. Should there be differentiated retention for those convicted of different offences?
    5. Alternatively, is there an evidential way to decide how long the biometrics of those convicted need usefully to be retained?[53]
    6. Should the police have access to biometrics taken and retained by others? For example, facial images on social media sites? Apart that is (as is currently the case) for controlled access to those of foreign law enforcement agencies under joint treaty arrangements.

77. Third, is the question of trustworthiness: that is how can the public be confident that the use of biometrics will be in their collective interest and respect their privacy? The brief answer is through legislation but that begs the question of how:

    1. Are there technical solutions that will enable transparency of AI-driven algorithms so that we understand how they are working and understand their flaws? If not, should legislation restrict any operational or evidential role in criminal trials until such solutions are available?

53 For an example of this approach see: R. Dubourg and I. Vincent: DNA Retention Policy: results of analysis relating to the protections of 'the Scottish model', Home Office Research Report 58, 2011.

2. Should legislation govern the taking, retention and use of new biometrics in the same way that already applies to the police use of DNA and fingerprints? If not, how can different rules be justified?
3. Should there be sanctions against breaches of the legislative rules for the use of biometrics? Does that need a regulator?
4. Does the need for trustworthiness require that there be a mechanism within new legislation that provides independent oversight of the legislative regime, which requires public reporting?

78. Fourth, are questions about individual privacy:

1. Any police use of new biometrics will be a limitation on individual privacy and raises questions about proportionality. How will that be decided? In the principles of the legislation or, if not, by a subsequent mechanism? Should that mechanism be national or local?
2. Should individuals have the right to challenge police holding or use of their biometric? If so, can any such mechanism be made more useable than present arrangements that apply to police holdings of DNA, fingerprints and custody images? Should the decision making be independent?
3. Should there be any constraints on the police trawling of biometrics (for example, facial images) available on the web, taken for non-policing purposes (for example, for social media)?
4. More generally, what do we think is acceptable in terms of intrusion versus privacy?

79. Fifth, are questions about access to databases:

1. How will police access to databases for which Chief Officers are not the data controllers be governed? How and by whom should such decisions be made?
2. Should any non-police body or agency have access to policing databases? How and by whom should such decisions be made?
3. How will government multi-user data platforms be governed to avoid abuse of any data sharing restrictions?
4. What rules should cover international access to UK biometric databases or exchanges of information from UK biometric databases in future? Who will be responsible for this governance?

80. Sixth, are questions about whether there ought to be different provisions for national security:

1. Should there be special provisions for the holding of a subject's biometrics for reasons of national security, which would not otherwise be possible under the governance of biometrics held for purposes of criminal investigation anywhere in the UK, similar to that provided in PoFA?
2. If such provision is made what oversight of this should be put in place and should it involve an independent person as in PoFA?
3. If such provision is made what are the roles of the police and of the British Security Service in decision making about biometrics?

81. These are some of the questions that any future governance rules or legislation will need to answer. The answers to the questions are also the issues that Parliament may wish to scrutinise in debating any future legislation.

82. Scotland's answer to these questions is to create legislation based on principles and then have a Scottish Biometrics Commissioner draw up an evolving Code of Practice for the use of biometrics based on those principles to govern the capture, retention, use and deletion of biometrics.[54] Initially the Code will apply to the police but with a possibility to later extend the range. The Scottish Commissioner will have a very different role from mine.[55] Given that Scotland is the first country to legislate[56] then it does offer a model for others, but the particularities of the Scottish situation mean that it might not be a model that will easily fit England and Wales. Where Scotland is a model for all, is in the kind of questions that they have sought to address.

83. Carrying out this work will be especially difficult if governments wait until they are forced into rapid action by public concern. In Scotland they started with commissioning a report from a group of stakeholders and experts, consulted on their report and drafted legislation before presenting a Bill to Parliament. This process took over two years but has meant that broad agreement and support has been built for the proposals.

THE STRATEGIC CHOICE

84. Deciding the future governance of biometrics is part of a much larger strategic political choice about our future. The technological changes that are resulting from AI-driven analytics will transform much more than biometrics. What is happening is another one of those technically disruptive process which fundamentally change the social world. Politicians in democratic countries have been slow to understand that a new world is emerging outside of their control.

85. However, that has not universally been the case and China recognised much more quickly the possibilities provided by new technologies, especially new biometrics, for social control, or as they interestingly refer to it for 'the rule of law'. It is because they see these possibilities that they have also set themselves the goal of becoming world leaders in developing such technology. What is noteworthy about China's use of biometrics is that it goes beyond controlling and sanctioning people's actions, to changing the way people think about the nature of social order. Attempting to re-make both the social order and citizens' thinking is clearly a politically strategic decision about what kind of world they regard as desirable in the future. I doubt that the Chinese choice will appeal to us simply because of the centrality for us of individual rights being a limitation on the exercise of politically organised social control. I mention what is happening in China not to shroud-wave, but only to illustrate the point that thinking about how the police should use new biometrics raises a bigger strategic question about what kind of political order and social world we wish to see come out of this new period of technological disruption?

86. In conclusion, as a society we are just emerging out of a period where technical change was regarded as inevitable to an understanding that some of the early products of the new technologies are of dubious value or in some cases positively harmful either to individuals or social life. As in earlier times of technological disruption, we can manage that process if we

54 Matters of national security are not devolved and so the Scottish Bill only deals with police use of biometrics for criminal investigations.
55 For more details about the Scottish provisions see https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx
56 Although other countries are examining legislation for the police use of new biometrics. See:https://www.biometricupdate.com/201510/hungarian-government-proposes-storing-biometric-data-of-citizens

choose. Working out how to provide governance for the new technologies will be difficult since some of them operate beyond the nation state, although the state remains the source of law and a rules-based international system. Legislating for new biometric use by the police is a juridical problem but the primary question is what kind of social and political world do we want the new technology to create? It might not be easy to reach political agreement on that question but answering such questions is the point of politics. The debates are necessary since the outcome will be expressed through legislation about the police use of biometrics.

3. BIOMETRICS FOR LAW ENFORCEMENT IN ENGLAND AND WALES

87. The Protection of Freedoms Act 2012 (PoFA) was unusual in that it created the role of Biometrics Commissioner. The Commissioner has some decision-making powers in relation to applications to retain biometrics made under section 63 of PACE and the awarding of National Security Determinations. In addition to these powers the Commissioner is responsible for keeping under review the retention and use of DNA and fingerprints by the police and for reporting annually to the Home Secretary on compliance with the relevant provisions of PoFA. 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. In this chapter I deal with the discharge of those powers and responsibilities in relation to law enforcement or what might be referred to 'the policing of general crime' by police forces and other law enforcement bodies in England and Wales[57].

OTHER INDEPENDENT OVERSIGHT OF BIOMETRIC USE BY THE POLICE

88. 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.[58] 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.

89. 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.[59]

90. The Data Protection Act 2018 (DPA) updated data protection laws governing the processing of personal data for law enforcement by the police and others. Part 3 of the Act concerns law enforcement and under that Part the processing of biometrics under the Act is considered to be "sensitive processing"[60]. The DPA sets out six data protection principles which apply to law enforcement processing of data, it sets out the right of individuals over their data and it also places restrictions over those rights, but only where necessary and proportionate to do so. The Information Commissioner's Office, headed by the Information Commissioner Elizabeth Denham, is an independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals[61].

i. PoFA regulation of DNA and fingerprints

91. The police usually have the power to take a DNA sample (usually by way of a swab inside the person's cheek) and a set of fingerprints, without consent, from every person that they

57 The responsibility to oversee National Security Determinations and the biometric retained under such determinations is UK wide as national security is not a devolved matter. The discharge of these UK wide responsibilities is dealt with in chapter 4 of this report.
58 See http://www.gov.uk/government/organisations/forensic-science-regulator
59 See https://www.gov.uk/government/organisations/surveillance-camera-commissioner
60 Data protection Act 2018, Part 3, s. 35(8)(b)
61 https://ico.org.uk/

arrest[62]. Fingerprints are much quicker and cheaper to process and use than DNA. Further, the way fingerprints are searched and used by the police, is different from their use of DNA (see also paragraphs 101 to 104 below). 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 held on the National DNA Database (NDNAD).[63]

RETENTION RULES

92. 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;[64]
- that if an individual is convicted of a recordable offence their biometrics (DNA profile and/or fingerprints) may be kept 'indefinitely';
- that if an individual is charged but not convicted for certain more serious offences (called 'qualifying offences'[65]) 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.

93. 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

62 Police and Criminal Evidence Act 1984 (PACE) s. 61 and s. 63.
63 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 older SGM or SGM plus chemistries the profile already held may require upgrading using the current DNA-17 profiling method, in which case another DNA sample will be taken.
64 That general rule recognises the extreme sensitivity of the genetic information that is contained in DNA samples.
65 See section 65A(2) of PACE. A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.

Non convictions

Alleged offence	Police action	Time period
All Offences	Retention allowed until the conclusion of the relevant investigation[66] 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) [67]

PROVIDING ASSURANCE ON POFA COMPLIANCE

94. In order to report on compliance by the police with the provisions of PoFA I and the team from my Office make regular visits to police forces and other law enforcement agencies. During 2018 we visited 24 territorial police forces. During the 2019 reporting period we visited another 20 territorial forces as well as the British Transport Police, the Ministry of Defence Police and the National Crime Agency. The purpose of the visits is not only to find out how forces are applying PoFA in a narrow sense but to build up a national picture of pertinent, wider issues related to the use of DNA, fingerprints and, increasingly, other biometrics. We aim through the visit programme to assist forces by talking through problems, advising where we are able to and sharing knowledge or best practice that we have observed elsewhere. Further, the fact of our visit often has the immediate effect of focusing forces on whether their procedures in relation to PoFA are adequate and compliant.

95. During the force visits I and my team typically speak with a range of police staff and officers, both senior and junior, including those who work in the force scientific or forensic services department[68], those who are responsible for custody and detention procedures and those who are responsible for information management, as well as those more directly involved in investigative work. Prior to the visit I ask the force to provide me with extensive information, including relevant policies, statistics and other evidence of current practices. The visit itself usually takes place on one day although we recently spent three days visiting the Metropolitan Police Service[69], given the size and reach of the force. Following each visit the force is provided with a short report containing recommendations relating to any areas where it is apparent that

66 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.

67 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.

68 Some forces have collaborated this service, for example the Yorkshire and the Humber forces have a collaborated forensic and scientific service situated in West Yorkshire and five East Midlands region forces all use the same central scientific services hub; EMSOU. In these cases we visit each force individually as well as talking to the staff in the collaborated service as despite such collaborations individual force practices vary.

69 This visit focused on the policing of general crime rather than CT policing, the oversight of which I have to date conducted separately for practical purposes.

the force need to think again about their approach to a particular issue or improve practices and procedures in a particular area. Many of these recommendations are common to a number of forces and some to almost every force, which highlights that those issues are proving problematic for forces nationally.

ii. Retention and use of DNA and fingerprints

THE GOVERNANCE OF NATIONAL DATABASES

96. The National DNA Database (NDNAD) was overseen by the National DNA Strategy Board (NDNASB), which was given a statutory role in PoFA.[70] In March 2016, fingerprints were added to the remit of the Board and it has become the Forensic Information 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[71].

97. 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[72], 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'. To date I have seen no concrete proposals in relation to this commitment and although I am aware that a review of governance began to be conducted by the Home Office during 2019 – indeed I was asked for my views as part of this review – this has now, I understand, been superseded by the transition to a new government and aforementioned manifesto commitment to *empower the police to safely use new technologies like biometrics and artificial intelligence, along with the use of DNA, within a strict legal framework*[73].

98. 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,[74] the Forensic Science Regulator, the Biometrics Commissioner, the Information Commissioner[75] and representatives of the devolved administrations.

---

70 See section 63AB of Police and Criminal Evidence Act 1984 (PACE) as inserted by section 24 of POFA.
71 See also Chapter 5, paragraph 307
72 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf
73 See also Chapter 2, paragraph 60
74 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
75 See http://www.ico.org.uk/

FIND-SB publishes an annual report which is laid before Parliament[76] 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

99. The National DNA Database (NDNAD) was established in 1995 and, by the end of the calendar year 2019, held 5,941,883 subject DNA profiles and 616,052 crime scene profiles for England and Wales. This equates to an estimated 5,092,995 individuals. UK holdings total 6,521,725 subject profiles and 644,710 crime scene profiles, or an estimated 5,575,69 individuals.

TABLE 2: Number of DNA profiles held (year ending 31 December 2019)

	Subject Profiles	Crime Scene Profiles	Total
England and Wales[77]	5,941,883	616,052	6,557,935
Rest of UK[78]	579,842	28,658	608,500
Total	**6,521,725**	**644,710**	**7,166,435**

Source: FINDS-DNA

TABLE 3: Total DNA Holdings on NDNAD by Profile Type (year ending 31 December 2019)

	Arrestee	Volunteer[79]	Crime-scene from mixtures[80]	Crime-scene from non-mixtures	Un-matched crime scenes[81]
England and Wales	5,939,826	2,057	121,258	494,794	194,417
Rest of UK	577,570	2,272	2,245	26,413	17,811
Total	**6,517,396**	**4,329**	**123,503**	**521,207**	**212,228**

Source: FINDS-DNA

100. 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, and to 123,503 in 2019) reflects the increasing ability of forensic scientists to analyse such complex stains over recent years.

76 https://www.gov.uk/government/publications/national-dna-database-annual-report-2017-to-2018 The 2018 to 2019 report has not to date been published.
77 Includes British Transport Police.
78 Includes Scotland, Northern Ireland, Channel Islands, military police forces and Customs and Excise.
79 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.
80 Mixed profiles include the DNA information of two or more persons.
81 The number of unmatched crime scenes is included in the crime scene from mixtures and non-mixtures figures.

NATIONAL FINGERPRINT DATABASE

101. 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 began enrolling tenprints in 2013. Presently, fingerprints taken under PACE or its equivalent in the UK are enrolled onto IDENT1 for storage and search.

102. The present Livescan[82] 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).

103. Unfortunately the statistical information available about the holding and use of fingerprints has never been of the standard and detail as that available for the DNA database as it is essentially contract compliance data rather than the most useful management information. The figures provided below are therefore provided with the caveat that this is the best information currently available. I understand that as of the autumn of 2020 new supplier will run the IDENT1 system but that this will initially be on exactly the same basis as the service provided by the current supplier. Work is, however, underway to improve the standard of the available statistical information. In any event, for the time being the statistical information available continues to be poor and not fit for purpose.

104. IDENT1, as at 31 December 2019, held 26,018,045 sets of tenprints, which relate to 8,372,420 unique arrestee subject tenprint records (i.e. 8.37 million individuals currently have their fingerprints held in the main policing fingerprints collections on IDENT1) and 2,233,267 unmatched crime scene marks relating to 932,432 cases[83].

TABLE 4: Total Holdings on IDENT1 by classification (year ending 31 December 2019)

	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	24,860,672	Data not available	1,929,774	Data not available
Rest of UK	1,157,373	Data not available	303,493	Data not available
Foreign convictions	Data not available	Data not available	Data not available	Data not available
Total	**26,018,045**	**8,372,420**	**2,233,267**	**932,432**

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

82 Livescan is an electronic fingerprint capture system for capturing subject fingerprint and palm print data for enrolment onto the database.
83 This data is for the main policing collections on IDENT1.

ADDITIONS TO NDNAD IN 2019

105. The number of DNA subject profiles being added to the database has declined over recent years, for example numbers have declined from 540,100 profiles added in 2009/10 to 265,562 profiles added in 2019[84] [85]. There are thought to be a number of reasons for this, mostly linked to a decline in the number of arrests due both to reductions in policing resources generally and to the increased use of voluntary attendance for dealing with suspects rather than arrest. This is discussed further at paragraphs 125 to 133 of this chapter.

TABLE 5: Additions to NDNAD (year ending 31 December 2019)

	Arrestee	Volunteer[86]	Crime-scene from mixtures[87]	Crime-scene from non-mixtures
England and Wales	232,550	43	21,068	11,170
Rest of UK	33,012	83	400	1,104
Total	**265,562**	**126**	**21,468**	**12,274**

Source: FINDS-DNA

106. 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[88] and then increased to its present level of 6.52 million; this is in large part because the number of new profiles loaded has declined. The number of crime scene profiles loaded onto the database has declined from 50,000 in 2008/09 to 33,742 in 2019. This appears to be largely attributable to cuts in policing resources during recent years. During my visits to police forces 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.

107. In the fiscal year 2018/19, 117,430 subject profile records were deleted from the database[89] and 4,846 crime scene profile records were deleted.[90]

ADDITIONS TO IDENT 1 IN 2019[91]

108. During 2019, 867,994 unique arrestee records[92] and 28,749 crime scene cases were created on IDENT1. A total of 135,105 unmatched crime scene marks were added to the database although several marks will often be attributable to the same crime, hence the much lower number of new cases created.

84 The 2018 figure was similar, with 256,422 subject profiles added to the database during 2018.
85 Data supplied by FINDS-DNA. Special thanks to Caroline Goryll of FINDS-DNA for her help in preparing the relevant data.
86 '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.
87 Mixed profiles include the DNA information of two or more persons.
88 This was in part due to deletions required by the newly enacted PoFA legislation.
89 Including automatic 'PoFA' deletions and deletions under the 'Deletion of Records from National Police Systems' Guidance; see also paragraphs 163 to 166.
90 All these fiscal year figures are sourced from FINDS. Comparative figures are not available for calendar years due to ongoing issues with the management information that FINDS-DNA are able to obtain.
91 This data is for the main policing collections on IDENT1.
92 It is not possible at present due to the aforementioned constraints on obtaining data to ascertain how many individual subjects this relates to.

TABLE 6: Additions to IDENT1 (year ending 31 December 2019)

Tenprint sets from arrestees	Individual subjects	Unmatched crime scene marks	Cases created with unidentified crime scene marks [93]
867,994	Data not available	135,105	28,749

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

TABLE 7: Deletions from IDENT1 (year ending 31 December 2019)

Tenprint sets from arrestees	Individual subjects	Unmatched crime scene marks	Cases with unidentified crime scene marks
140,236	39,227	154,022	Data not available

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

109. During 2019, 39,227 individual PACE subject records and 154,022 crime scene marks were deleted from the database. Deletions of subject records 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. Unidentified crime scene marks are removed from the database once they have been identified and that identification has been verified[94].

SPECULATIVE SEARCHES

110. The police have the right to make a speculative search of a DNA profile or fingerprints against existing holdings on the national databases *within such time as may reasonably be required for the search*[95]. In practice, for fingerprints this is usually done automatically as soon as, or shortly after, the arrestee's fingerprints are taken in custody and the result is usually returned almost instantaneously. This is because there is an automated search function provided by Livescan machines, which communicate directly with IDENT1, which allow tenprint sets to be immediately searched against one or more collections of fingerprints on that database, including the cache containing unidentified crime-scene marks. This can be useful to confirm the identity of the individual who has been arrested if their fingerprints are already held on the national database. Further, potential matches with unidentified crime-scene marks can be made at this point, although these then need to be checked by fingerprint experts.

111. For DNA the process is slower as the DNA sample taken from the arrestee in custody must be sent to a laboratory for the profiling before it can be loaded to the NDNAD and searched against existing profiles. Nevertheless, the speculative search is still useful as the search is also against existing holdings of unidentified crime-scene DNA profiles, to determine if there is a match.

112. The right to make a speculative search is particularly important in circumstances where an arrestee without previous convictions is quickly released with no further action taken against

93 Cases created may not be filed to the database.
94 Or the case is required to be deleted according to the Management Of Police Information (MOPI) rules.
95 PACE 1984 section 63D(5)

them (NFA'd) and their biometrics therefore fall to be deleted. This is most significant where the individual has come to police attention for the first time.

MATCH RATES – DNA

113. 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. For the reasons highlighted in paragraph 106 above this is increasingly so based on available resources.

114. Given that most of those convicted of a recordable offence will have their DNA and fingerprints retained,[96] biometrics will be available to police investigators for most of those who reoffend. Repeat offenders make up a significant proportion of overall offending. As a result the rate at which crime scene profiles produce a match to subject profiles held on the database is high (presently 67.65% for England and Wales in 2019 which is fractionally lower than last year).

TABLE 8: Match Rate for Matches obtained immediately on loading for England and Wales Forces (year ending 31 December 2019)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	32,238	232,549
No. of Matches	21,808	4,791
Match Rate	67.65%	2.06%

Source: FINDS-DNA

TABLE 9: Match Rate for Matches obtained immediately on loading for all UK forces (year ending 31 December 2019)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	34,012	265,561
No. of Matches	22,217	5,315
Match Rate	65.32%	2.00%

Source: FINDS-DNA

MATCH RATES – FINGERPRINTS

115. The match rate for fingerprints and palm prints, compared to that for DNA, is currently difficult to calculate in a meaningful manner for the aforementioned reasons related to the availability of data. Nevertheless, match rate ratios are now produced by the FINDS – National Fingerprint Office on a monthly basis. The ratios are the number of searches performed for each (1) declared identification.

96 Whilst PoFA would allow all such biometrics to be retained (with the exception of biometrics from those aged under 18 in some limited circumstances), biometrics are not necessarily taken in all such cases.

TABLE 10: Fingerprint matches during 2019

	Scene of crime palm mark to palm print	Scene of crime fingermark to tenprint	Tenprint to scene of crime mark
Total searches	81,818	446,571	Data not available
Number of matches	4,455	187,88	Data not available
Match rate	1:18.4	1:23.8	1:142.69

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

iii. Footwear Impressions

116. Footwear impressions are not a biometric but nevertheless they are included in PoFA. Section 15 of PoFA[97] 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."*[98]

117. There are two national footwear databases, both of which are run by FINDS: the National Footwear Reference Collection (NFRC) and the National Footwear Database (NFD).

118. The NFRC is essentially a catalogue of pattern codes for different types of footwear which has been developed by coding footwear impressions found at crime scenes and footwear impressions taken from arrestees and attributing a code to each unique pattern. Only the image of the footwear impression is added to the NFRC. No information about the individual to whom the shoe was attributed is recorded.

119. The NFD is an intelligence tool and is used to hold records of footwear patterns encountered at both crime scenes and on footwear impressions taken from people in custody. A pattern code from the NFRC can be allocated to both types of marks and recorded on the system; this can then be used to link scenes to scenes or scenes to suspects.

120. In previous years I have reported that there is no agreed national policy or even approach being applied to the retention of footwear impressions by all police forces in England and Wales[99]. Indeed, not all forces routinely collect footwear impressions. Some forces upload the images of marks from scenes to the NFD and others upload images of the prints taken from footwear. Others record the pattern code and do not upload images. The length of time for which footwear impressions are retained varies depending on the use made of those impressions and whether they can be attributed to an individual. Whilst some forces upload their footwear impressions onto the national databases many do not.

121. There is no national data available on the use made of footwear impressions and the outcomes. Anecdotally, some forces tell me that they see little benefit in taking and processing footwear impressions whilst others claim to have seen excellent results from doing so. In addition, a

97 Which amends section 63F of PACE.
98 See: http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/1/enacted.
99 Although oversight of the NFD is now part of the NPCC portfolio and discussed at the expanded National Fingerprint Board which changed as of January 2020 to the National Fingerprint and Footwear Strategic Board.

number of forces are re-examining their use of footwear impressions as part of their review of their budgets.

iv. Other issues affecting the taking and retention of DNA and fingerprints

122. Whilst PoFA provides a specific legal framework for the police retention and use of biometrics (DNA and fingerprints), other changes to legislation and associated statutory codes have had significant consequences for both the taking and retention of biometrics, which I have previously referred to as 'unintended consequences'. These have been highlighted in previous Annual Reports by both myself and my predecessor. Whilst these do appear to be unintended consequences this does not mean that they could not have been foreseen. As I have pointed out repeatedly they might well have been anticipated if the Home Office fully considered the operational consequences of the proposed changes 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.

123. Most significantly, in my view, the police ought to be provided with guidance as to the precise interpretation of new legal frameworks and how these are intended to be implemented. Instead, what we have seen repeatedly, including following each of the changes outlined in this section, 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.

124. Two changes that appear to continue having a significant effect are:

A. 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[100]. 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.

B. 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[101].

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

101 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.

A. VOLUNTARY ATTENDANCE[102]

125. Since the 2012 changes to Code G 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, usually outside of a custody suite[103], to answer police questions and are commonly known as 'voluntary attendees' (VAs).

126. During the visits made by my Office to police forces in England and Wales over the past two years there have been extensive discussions about the use of voluntary attendance (VA). Whilst forces report that their move from arrest to VA was initially driven by the changes to Code G most also cite reasons that are related to increasing financial pressures including: rationalisation of custody estates[104], problems of geography and distance to a custody suite and the burden (both in terms of time and administration) of taking someone into custody. Essentially there are significant cost and time savings for stretched forces and individual officers using VA, thus a further pull factor in favour of using VA rather than arrest.

127. 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 VA. 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.

128. In many cases the use of VA 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.

129. I have observed the following problems in relation to the current use of VA:

    a. VA is being used for a wide variety of offences, including sexual offences (including rape), some of which may be inappropriate. Without arresting the suspect biometrics cannot be taken at the outset and a speculative search of the subject's biometrics cannot be made where in fact it may be appropriate or necessary as part of the investigation.

    b. 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 and the wider community caused by this is not always being fully assessed and/or mitigated.

102 For a more detailed account of the causes and problems of voluntary attendance see Chapter 3 of my 2018 Annual Report https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812351/Biometrics_Commissioner_AR_2018_Print.pdf

103 Suitable recording equipment must be used to record the interview which may be static or mobile. 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.

104 The increasing use of voluntary attendance has had the concomitant effect of reducing the flow into custody suites so reducing their economic viability.

c. Although national guidance is now available that clarifies when it is appropriate and lawful to obtain biometrics from VAs there remains some confusion about this. In any event, many forces have no effective procedures in place to ensure that opportunities for capturing biometrics from VAs are taken.

130. As to the third of these observations NPCC national guidance now states that biometrics should be taken only if the VA is cautioned or charged at the time of their interview, or if they are subsequently issued with a notice of intended prosecution (frequently a postal charge). That guidance, however, is somewhat lengthy and legalistic and has not, therefore, been as useful as it might have been. There has also been a problem with the distribution of the guidance with many forces unaware of its existence or unable to locate it[105]. There also remains a practical problem that the opportunity to lawfully take biometrics frequently occurs long after the suspect has left the police interview. Further, it appears that some police forces currently have no process for identifying suspects from whom they may lawfully obtain biometrics. Finally, although many forces have started to send letters to VAs, together with the postal charge, asking them to attend for biometric capture there are a number of practical difficulties with ensuring that this actually takes place and in some forces uptake is very low.

131. The overall effect of the above factors is an inconsistent picture nationally and, in my view, both the appropriate use of VA and biometric capture from VAs continues to be a significant problem for most police forces. At the same time there has been a general reduction in the taking of biometrics and therefore in additions to the national biometric databases. 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.

132. Those who have read my 2018 Annual Report will notice that unfortunately little has changed over the past 12 months in terms of the national picture in relation to VA. On a local level, however, I am pleased to report that there has been some improvement. 75% of the police forces visited during 2018 required a process to be put into place to ensure that biometrics were captured from VAs once there was a lawful basis for doing so. It was my recommendation that they implement such a process. Over half of these forces responded a year later stating that they were well on the way to implementing measures to address this issue. Of the forces that we visited during 2019 many were already some way towards implementing such a process or had at least identified the gap. Very few, however, had fully implemented such processes, including a very large police force who account for a significant proportion of crime nationally.

133. There are possible counter measures to these risks. Some forces 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 consent and the necessity and proportionality of such a power. Another possibility would be to provide further guidance on the interpretation of Code G of PACE, encouraging officers to think very carefully about

105 For a further discussion of the problems with guidance for the police see also paragraphs 137 to 139 below.

whether to arrest a suspect if there is a possibility that taking biometric samples would provide evidence of the person's involvement in the offence at issue or other related offences.

B. BAIL AND 'RELEASED UNDER INVESTIGATION'

134. 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).

135. 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. My Office have questioned forces about the effect of the changes during our visits and unfortunately it appears that my fears have come to fruition and in many cases RUI cases have been protracted and have not been monitored efficiently. In addition, many forces faced IT challenges in implementing the changes and have been unable to rapidly update their systems. This means that in many forces the PNC record[106] is not automatically updated when an investigation has ended[107] which is significant as it is the updating of the PNC record that causes biometrics to be deleted from the databases where appropriate. As a result, there may be unlawfully held biometrics, which if the systems had worked correctly would have been deleted.

136. 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"[108]. 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, the police and others have highlighted risks to victims caused by the decline in the use of bail. The government now appear to recognise the problems that have been caused by this change and have launched a public consultation on this matter "in recognition that more needs to be done to ensure cases are dealt with effectively"[109]. I hope that as part of this consultation they will listen to those in the police force at an operational level who must work with whatever new system is to be implemented following the consultation and also take time to consider any 'unintended consequences'.

106 PNC is the Police National Computer. It contains a record of all arrests, charges and convictions, together with demographic information. There is a link between PNC, IDENT1 and the NDNAD so that if, for example, a suspect with no previous convictions is NFA (no further action is to be taken against them) PNC will automatically cause the biometrics to be deleted from the databases,

107 Including one large force who currently have over 40,000 open cases on the PNC which need to be updated.

108 https://www.gov.uk/government/news/28-day-pre-charge-bail-limit-comes-into-force

109 https://www.gov.uk/government/news/government-launches-public-consultation-on-pre-charge-bail

LEGISLATION AND GUIDANCE

137. In relation to VA it took over six years for national guidance to be issued to advise the police about when they might lawfully take biometrics from VAs. In relation to the changes in bail legislation it took over a year for guidance to be issued and in relation to use of the CPIA exception to retain DNA samples beyond six months in contravention of PoFA guidance has still not been issued[110]. It appears that part of the reason 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. 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. Even in relation to PoFA, which was enacted in 2013, some promised guidance has still not been issued[111] despite the Minister with responsibility for biometrics repeatedly stating that guidance would in future be produced in a timely manner[112].

138. The issue of guidance is also a more general one. Currently there is no one place where police officers are able to access guidance as some guidance is issued by the College of Policing, some is issued by the NPCC and some by the Home Office. Each of these bodies may variously put the guidance on their website, distribute it by email or distribute it via some other internal means of communication. Further, there appears to be little in the way of editorial function or style guidance so guidance may be out of date or difficult for operational officers to understand or follow. These problems are compounded by the sheer volume of information that police officers are now expected to take on board in order to perform their duties correctly and lawfully. Were there to be a single, accessible repository for guidance, which contained guidance that was up to date and written in way that was easy to understand and to implement operationally that might assist somewhat.

139. In any event, in future 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

110 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.

111 No guidance has yet been issued on the meaning of 'indefinite retention', the CPIA exception 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.

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

period of confusion, often followed by non-compliance and a number of unintended, potentially damaging consequences.

v. Processing and storage of DNA samples

SAMPLING ERRORS

140. After a DNA sample has been taken from an arrestee in custody that sample will be collected and taken to the force's own (or collaborated) scientific or forensic service for checks to be made such as whether the bag has been properly sealed, the barcode has been correctly applied and the swab has been correctly placed in the tube. The sample is then submitted to a Forensic Service Provider (FSP) for profiling. FSPs also 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[113] that are found in the processing of DNA are generally acceptable for example sampling and record handling errors by FSPs are made in relation to just over 0.0057% of subject profiles. Errors are made by FSPs when interpreting subject profiles in less than 0.0038% of cases and in interpreting DNA profiles from crime-scenes in relation to around 0.19%.[114]

141. Since April 2016, data has been collected for FIND-SB on errors in DNA sample handling errors by police forces, both at crime-scenes and in custody. This year, for the first time, all forces provided data on errors identified in force and those errors have now been categorised in a uniform way. It is therefore possible to draw some conclusions from the reported errors; for example, by far the most common error during 2019 was failure to seal the bag containing the DNA sample. Following recommendations made to them following previous visits the majority of forces now have procedures in place to monitor errors, identify patterns and inform the need for further staff training where necessary. Administrative errors may also occur which mean that profiles cannot be loaded to the database. In England and Wales around 0.7% of profiles cannot be loaded for this reason. Samples may also be lost by forces and although these are again, very small in number (around 0.8% of samples); it is worrying however that some forces have not been able to report to FINDS the number of 'lost samples' this year[115]. 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[116]. These errors occur in around 0.07% of all subject profiles loaded to the NDNAD.

142. 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.[117] On visits to police forces we have found that procedures for re-sampling vary but not all forces have defined processes for reporting failed samples and ensuring that the sample is re-taken. Some forces only re-take samples in

113 (i.e. the number of errors found through the DNA supply chain from sampling to matching against the NDNAD)
114 Figures are for 2019. Previous Reports contained figures for fiscal year 2017/18. Source: FINDS-DNA.
115 Bedfordshire, Cambridgeshire, Hertfordshire, Greater Manchester, Surrey, Sussex and Thames Valley Police have not been able to provide this data to FINDS.
116 These occur when the DNA profile is associated with the wrong information.
117 At the very least additional police resources are needed to re-take the sample from the subject (who may well have left police custody).

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. On a more positive note of the forces visited in 2018 I recommended to 75% that more formal processes needed to be established in following up DNA sampling failures. Of those to whom that recommendation was made the majority reported a year later that they had put in place policies to address this issue or re-visit this area.

143. 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.

FORENSIC SCIENCE PROVIDERS

144. In England and Wales services such as the profiling of DNA samples and the matching of DNA profiles from crime scenes to profiles are provided to police forces by three private forensic science providers: Key Forensic Services (KFS), Eurofins Forensic Services (EFS) and Cellmark Forensic Services (CFS). There have been some serious concerns, particularly over the past three years, about the stability of the forensic market place in England and Wales. Dr Gillian Tully, the Forensic Science Regulator, has raised these concerns repeatedly with the Home Office and others and in her Annual Reports. She reported this year that concerted effort by a police-led Market Stabilisation Gold Group has prevented a market collapse in the short term, but concerns remain about long term viability[118]. In Scotland and Northern Ireland similar forensic services are provided by the Scottish Police Authority Forensic Service and Forensic Science Northern Ireland.

145. During 2019 a cyber-attack on EFS had a highly detrimental effect on the entirety of the forensic market. As a result, there were long delays in processing PACE DNA samples with a subsequent risk that searches of newly profiled samples against the NDNAD were carried out many months after the samples were taken. This served to illustrate the fragility of the current setup and its vulnerability, particularly were one of the three providers to be absent from the market for a prolonged period or on a permanent basis in future.

DESTRUCTION OF DNA SAMPLES

146. There are clear rules in PoFA as to when biometric samples should be destroyed.[119] 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

118 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868052/20200225_FSR_Annual_Report_2019_Final.pdf page 11.

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

is an exception under the Criminal Procedure and Investigations Act 1996 (known as the CPIA exception) [120].

147. 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.

148. From the visits carried out to 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 EXCEPTION

149. 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"*.[121] In such circumstances, the sample may be retained until it has fulfilled its intended use (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. [122]

150. 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.

151. 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).

120 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.

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

122 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.

152. Since January 2016, all elimination samples have been subject to the same retention rules as those taken from individuals arrested for recordable offences.[123]

153. 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.

154. 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"*[124].

155. 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.[125] 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.

156. We found on our visits to police forces both last year and 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[126]) will be necessary this is not generally applicable to samples taken in relation to all sexual offence allegations. This is because DNA analysis is not usually relevant to the issue of whether the victim consented to sexual activity, which is the key issue in the majority of sexual offence allegations I have recommended to these forces that they urgently revise their policies. Unfortunately, only half of forces to whom I made this recommendation in 2018 had changed their policies a year later.

157. 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, as I was last year, is in relation to elimination DNA samples.

123 For further discussion of volunteer samples see: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016, 226-231.*
124 Ibid at paragraph 181.
125 A copy of this letter can be found in an Appendix D to last year's Report.
126 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

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.

158. 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 2019. These are set out below (Table 11). 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 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 to FINDS as requested[127].

TABLE 11: DNA samples held under CPIA by England and Wales forces (year ending 31 December 2019)

	Total		Held in Force		Held by FSPs	
	2018	2019	2018	2019	2018	2019
Arrestee/ PACE samples	6,952	7,070	1,190	899	5,762	5,880
Elimination samples	6,290	3,796	3,331	2,526	2,959	1,270

Source: FINDS-DNA

COPIES OF DNA PROFILES AND FINGERPRINTS

159. 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).

160. 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[128] or in case files, I have no reason to suspect significant non-compliance with section 63Q of PACE.

161. 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

127 For the second year Kent and Essex Police have not provided any figures for their end of year in force holdings, neither this year have Bedfordshire Police, British Transport Police, City of London Police or West Midlands Police.

128 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.

each of them appears to have in place proper processes to ensure the identification of hard copy fingerprints which should no longer be retained.

162. During 2018 I became aware 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[129]. I continue to be 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 continuing to keep this matter under close review.

vi. Deletion of police records ordered by Chief Constables

163. 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). The PNC contains records of arrests, charges and convictions relating to an individual together with their biographical details. It is the PNC that is commonly used to check whether an individual has a relevant 'criminal record', for example in relation to employment checks. 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[130] 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.

164. 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.

165. 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[131] 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

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

130 Where no further action has been taken against them following an arrest.

131 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

seems to me that whether a request for deletion will be approved remains somewhat a postcode lottery.

166. During the year ending 31 December 2019, 678 such deletions were approved by Chief Officers (see Table 12 below). This is compared to 612 such deletions approved by Chief Officers the previous year. Whilst 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. I also note the larger number of decisions pending with forces this year, which is possibly reflective of the stretch to police resources which is frequently reported to me by forces, particularly in the area of information management.

TABLE 12: Records Deletion Process (year ending 31 December 2019)

	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
2018	1,865	612[132]	609	499	140
2019	2,230	678[133]	621	435[134]	488

Source: ACRO Criminal Records Office – Records Deletion Unit

vii. Custody images

167. The police take a 'custody image' from every person they arrest and use these 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[135].

168. The Home Office eventually responded to this judgment by publishing, in 2017, a Review of the Use and Retention of Custody Images[136]. 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[137] (see also paragraph 173 for a discussion about PND). Rather than introducing a scheme for the automatic weeding of images to match the proportionality required by the judgment, the Review essentially reiterated that the time

132 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.
133 Of these 31 were approved for partial deletion. Of the 678 approvals and partial approvals 283 of these had a biometric element included as part of the deletion.
134 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.
135 *R(RMC and F) v Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin)
136 https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention
137 Retention on PND is a reflection of the retention of custody images held locally.

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. Over the past couple of years I have questioned whether the Review's proposals would withstand further court challenge.

169. 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[138]. The recommendations implement the guidance given in the Review but are quite restrictive and depend largely on the discretion of the Chief Officer. Over the past two years we have visited all of the police forces in England and Wales and we have found that there have been very few applications requesting deletion and therefore few deletions. Where custody images are deleted it is most often as a result of the ACRO records deletion process[139] as the application form for that process now includes a 'tick box' for custody image deletion.

170. We also found that police forces throughout England and Wales are finding it difficult to review the retention of custody images in line with the current MOPI requirements as the process is largely manual and very time consuming with current IT systems. As a result, few such reviews are being carried out, except where an individual requests such a review. Some forces are making attempts to carry out some deletions, for example by deleting in bulk very old custody images and a few are actually carrying out the active reviews required by MOPI but most are still retaining indefinitely the vast majority of their custody images, regardless of whether the individual has been convicted of an offence. 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.

171. The House of Commons Science and Technology Select Committee concluded in their report on 'the work of the Biometrics Commissioner and the Forensic Science Regulator' published in July 2019 that:

> *'progress has stalled on ensuring that the custody images of unconvicted individuals are weeded and deleted. It is unclear whether police forces are unaware of the requirement to review custody images every six years, or if they are simply 'struggling to comply'. What is clear, however, is that they have not been afforded any earmarked resources to assist with the manual review and weeding process. The Minister previously promised improvements to IT systems that would have facilitated automatic deletion. Such improvements now appear to have been delayed indefinitely. As such, the burden remains on individuals to know that they have the right to request deletion of their image. As we stated in 2018, this approach is unacceptable and we agree with the Biometrics Commissioner that its lawfulness requires further assessment.'*[140]

172. No details have been revealed of how automated deletion would be facilitated by any such IT improvements and I am given to understand that the Home Office are currently reviewing the

138 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
139 See also paragraph 163 above.
140 https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197006.htm#_idTextAnchor021

Custody Images Review, but I have been provided with no further details of what that review might entail.

viii. HOB databases and LEDS

173. Following the Bichard Inquiry Report[141] 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. 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. Presently PND contains almost 21 million images[142] of which around 17 million are technically suitable facial images of sufficient quality to be searchable[143]. It later transpired that one of the reasons why the Home Office had 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 twice confirmed by the Minister hearings before the Science and Technology Select Committee[144].

174. 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 facial image database also needs to be able to interact with police data on 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.

175. 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) with the single Law Enforcement Data Service (LEDS). I understand that there have been significant problems with NLEDP and that a 'stepping stone' approach is now being taken, meaning that delivery of full LEDS functionality is still many years away.

176. In the first instance the work being done by HOB will involve providing direct replacements for existing Home Office databases through providing a new, single supplier support contract for Home Office databases to be hosted on a generic biometric platform. For example, the police fingerprint databases and the immigration fingerprint database will both be hosted on the new platform. In the future the new data platform could also host other government biometric databases. The individual collections on the 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 business rules for each database. However, these practices vary as to whether their basis is found in

141 Dera.ioe.ac.uk/6394/1/report.pdf
142 This includes images of marks, scars, tattoos and some low-quality images that cannot be searched.
143 Figures provided by PND Service Desk.
144 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 She appeared again before the Select Committee on 19 March 2019 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.html

legislation or not and how access for third parties can be agreed. Before the data platform is 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 Home Office Biometrics Strategy[145] 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.

177. 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. 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 platform comes into wider use.

ix. Applications to the Commissioner to retain DNA and fingerprints (s 63G)

178. 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'[146] but neither charged nor convicted.[147] 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.[148]

179. 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.[149]

180. 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

181. From when the relevant sections of PoFA came into force on 31 October 2013 to 31 December 2019, 635 such applications to the Commissioner were received. Of those applications:

145 https//assets.publishing.service.gov.uk/.../Home_Office_Biometrics_Strategy_-_2018
146 Generally more serious violent, sexual offences, terrorist offences burglary and robbery. See: The Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013.
147 Under section 63G of PACE as inserted by PoFA.
148 Under section 63G(4) of PACE.
149 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.

- 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
- 65 applications were submitted in 2019[150]

182. In the last year, the number of cases submitted to my office has decreased to between 5 and 6 per month. However, during 2019 20 different forces made applications, which is the largest spread of forces since the inception of the process. Many of these forces made only one or two applications.

183. 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 31. 12 forces have yet to make an application – see further Table 13. During 2019 the MPS made 11 of the 65 applications to the Commissioner, with the other 54 made by 19 different forces.

184. The reduction in the number of applications made by the MPS this year to only 11 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 still experiencing with updating PNC at the end of an investigation, so by the time the Unit receives cases to consider they are already outside the 28 day application period (see also paragraph 135 above).

150 Different time periods have been used from previous annual reports, to better reflect the number of cases received by the OBC per calendar year.

TABLE 13: Number of Applications to the Commissioner by Force (Year ending 31 December 2019)

Force	2019	Total Applications since 31 Oct 2013
Yorkshire and Humberside[151]	14	69
Metropolitan Police	11	365
Essex	9	16
Hampshire	5	5
South Wales	4	17
Durham	3	4
Thames Valley	3	21
Avon and Somerset	2	5
Cleveland	2	4
Gwent	2	3
Hertfordshire	2	8
Northamptonshire	2	2
Northumbria	2	21
Cambridgeshire	1	14
Cumbria	1	2
Devon and Cornwall	1	16
Dorset	1	9
Bedfordshire	0	6
Derbyshire	0	1
Gloucestershire	0	1
Greater Manchester	0	3
Kent	0	26
Lincolnshire	0	1
Norfolk	0	1
North Wales	0	4
Warwickshire	0	4
West Mercia	0	6
Wiltshire	0	1
TOTAL	**65**	**635**

185. In the six years since the introduction of the PoFA Regime on 31 October 2013 (i.e. to 31 December 2019), applications to the Commissioner were received and determined as follows.

151 Collaboration on biometric retention consisting of Humberside, North Yorkshire, South Yorkshire and West Yorkshire.

TABLE 14: Applications to the Commissioner to Retain Biometrics for Qualifying Offences Under s63G PACE

	31 October 2013 to 31 December 2018	1 January 2019 to 31 December 2019
Total Applications	**570**	**65**
– Representations from subjects	69 (12%)	4 (6%)
Concluded by end of 2019[152]	**541**	**73**
Approved	350 (65%)	58 (79%)
Rejected	130 (24%)	12 (18%)
Withdrawn	61 (11%)	3 (4%)

LEGAL BASIS FOR APPLICATIONS TO THE COMMISSIONER

186. 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).

187. Between 31 October 2013 and 31 December 2019, 379 applications were made in relation to victim characteristics and 256 were made for the more general purpose of the prevention or detection of crime.[153] In a number of the former, more than one of the 'victim criteria' were satisfied.

TABLE 15: Statutory Basis for Applications to the Commissioner (31 October 2013 – 31 December 2019)

	Applications received[154]	Approved	Refused[155]
Victim criteria[156]			
– under 18	287	176	109
– 'vulnerable'	32	20	11
– associated with subject of application	86	29	56
Prevention/detection of crime	**256**	**185**	**71**

152 Cases concluded during 2019 do not correlate exactly with cases received in 2019 as there is necessarily a time lag between receiving and concluding a case.

153 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.

154 Including cases invalid or withdrawn; some cases are yet to be determined

155 In some cases more than one of the victim criteria are satisfied. For this annual report, all victim criteria have been considered in their own right, which shows a higher proportion of rejected applications when the victim is associated to the subject.

156 Cases concluded during 2019 do not correlate exactly with cases received in 2019 as there is necessarily a time lag between receiving and concluding a case.

PRELIMINARY APPLICATIONS

188. 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.

189. In fact, matters of disclosure have arisen only relatively rarely and to 31 December 2019 only 16 such applications have been made. All bar one of these preliminary applications have gone on to become full applications.

APPLICATIONS TO A DISTRICT JUDGE

190. 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.[157]

191. 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

192. 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.

193. 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.[158] 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.

194. 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'.

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

158 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?

195. 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 FIND-SB called Applications to the Biometrics Commissioner under PACE.[159]

196. 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;[160] or
- charging the subject would not be in the public interest.[161]

197. 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'.

198. 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.

199. 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,

159 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).

160 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.

161 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.

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.

200. 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*[162] that *'particular attention should be paid to the protection of juveniles from any detriment that may result from the retention … of their private data'*,

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

WHAT TYPE OF OFFENCES LEAD TO APPLICATIONS?

202. Only 'qualifying offences' can be the basis of an application but, as can be seen in Table 16, the majority (60%) of applications are for sexual offences.

TABLE 16: Outcome of Applications to the Commissioner to Retain Biometrics for Qualifying Offences under section 63G PACE (31 October 2013 – 31 December 2019)

Offence Group	Total applications	Approved	Refused	Withdrawn
Murder, Attempts and Threats to Kill	21	11 (52%)	6 (29%)	2 (19%)
Sexual Crimes	381	226 (59%)	113 (30%)	36 (9%)
Assaults	102	70 (69%)	11 (11%)	16 (16%)
Robbery	75	62 (83%)	2 (3%)	9 (12%)
Burglary	46	33 (72%)	11 (24%)	1 (2%)
Other	10	8 (80%)	1 (10%)	1 (10%)
Total[163]	**635**	**410**	**144**	**65**

203. 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.

204. 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

162 (2008) 48 EHRR 1169 at paragraph 124
163 16 cases from 2019 are still to be decided.

a more proactive approach to evidence building.[164] Conversely, the guidelines also advise that it may not be in the public interest to criminalise sexual behaviour, especially between young people[165], 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.

205. 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.

206. 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.

207. 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[166] and in any case the evidence refers to overall statistics and does not provide a basis for predicting the future behaviour of an individual.

208. 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.

209. 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. That analysis was published as Appendix E of my 2018 Annual Report. There were some limitations related to the time elapsed and the size of the sample of cases available but if this can be repeated 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.

164 See: https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-1-cps-policy-statement

165 https://www.cps.gov.uk/legal-guidance/youth-offenders. 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.

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

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

210. 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 17.

TABLE 17: Representations by Subjects and Outcomes (year ending 31 December 2019)

Applications	Totals	Representations made by the Subject of the Application
Approved Applications	408	41 (10%)
Refused Applications	142	27 (19%)

211. 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[167]. 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.

212. Subjects are given information about how to make representations when the police notify them about the application. Until recently this could only be done by the subject (or guardian/legal representative) writing to my Office. A review of this process carried out by my Office highlighted the need to simplify the instructions about how to make a subject representation and also to offer subjects the opportunity to telephone my Office, so that they can give their representation verbally should they wish to do so. The notification letter was revised so that it was easier to read. An accompanying note was also produced for subjects, which gives simple instructions about how to telephone my Office. The revised notification letter and accompanying telephone guidance note were circulated to some test forces at the end of 2018, and then to all forces in June 2019. Unfortunately, despite these changes, there has not been an increase in subjects making representations. To date, no subject has decided to telephone to provide representations. Whilst it is disappointing that the changes have not increased the number of subjects making representations, it is nonetheless important that these changes were made so that subjects are better informed about how they can make representations, should they wish to do so. Looking ahead, there are still other options to explore, which will be considered in the coming year.[168]

WRITING TO CHILDREN AND YOUNG PEOPLE

213. One unsatisfactory aspect of the application process that was introduced by PoFA, 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

167 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

168 These findings may also be relevant to the provision of government services more generally online or by telephone. Services in this form may be extremely difficult for some citizens to access, particularly where they have low levels of literacy.

(including children and young people[169]) 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.

214. In early 2019 this problem, having been looked at by various NPCC leads and police bodies for several years was passed to FIND-SB. A new policy was then decided upon and new guidance was produced, with input from my Office and other relevant parties, and the Chair of FIND-SB wrote to all Chief Constables in December 2019 informing them of the change of policy and new guidance. As a result, where an officer applies to extend the retention of a young person's biometric data, the officer will now contact the Youth Offending Team and/or Multi Agency Safeguarding Hub to identify the adult best placed to act in the young person's interests and provide support. As part of the application process, the young person will be made aware of the application and be additionally informed that the adult identified will be informed of the application. The young person will also be informed that the adult's contact details will be passed to the Biometrics Commissioner as part of the application process.

215. The above is, in my view, a much more sensible approach which safeguards both the safety of the children and young people concerned and protects their right to make representations to the Commissioner should they wish to do so. I am grateful to ACC Snuggs for his efforts in ensuring that this work was completed and that the new policy was adopted by the NPCC.

BIOMETRICS COMMISSIONER 'UZ' MARKERS

216. 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.

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

217. As of December 2019, a total of 186 UZ markers were in use by forces in England and Wales. That figure breaks down as follows:

TABLE 18: Biometrics Commissioner 'UZ' Markers by Force (January 2020)

Metropolitan Police Service	35
Northumbria Police	9
Durham Constabulary	2
North Yorkshire Police	1
West Yorkshire Police	18
South Yorkshire Police	3
Humberside Police	6
Cleveland Police	5
West Mercia Police	1
Warwickshire Police	2
Cambridgeshire Constabulary	8
Bedfordshire Police	9
Hertfordshire Constabulary	2
Essex Police	8
Thames Valley Police	10
Hampshire Constabulary	10
Kent Police	9
City Of London Police	3
Devon & Cornwall Police	8
Avon and Somerset Constabulary	1
Dorset Police	6
North Wales Police	1
Gwent Police	5
South Wales Police	24
Total	**186**

218. 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.

QUALIFYING OFFENCES LIST

219. My predecessor's 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.[170] 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. Not only does this affect the cases about which an application to the Commissioner for extended retention of biometrics can be made but it affects – in a potentially far larger number of cases – the automatic three year retention of biometrics for individuals charged but not convicted of a qualifying offence.

220. 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 despite repeated assurances from the Home Office over the past four years that it will be done.

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

4. BIOMETRICS AND NATIONAL SECURITY

221. 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 (MPS) Counter-Terrorism Command and in Northern Ireland by the Police Service of Northern Ireland (PSNI). The majority of counter-terrorism policing in the UK is carried out either by the MPS, the CTUs or PSNI, in coordination with National Crime Agency (NCA), Border Force, Ministry of Defence and Security Service.

OBTAINING BIOMETRICS

222. DNA samples (from which DNA profiles are derived) and fingerprints may sometimes be obtained in the course of investigations related to national security. In particular, biometrics may be obtained in the following ways[171]:

i The police may arrest a person suspected of having been involved in an offence directly or indirectly related to terrorism using their ordinary policing powers as set out in the Police and Criminal Evidence Act 1984 (PACE)[172] or similar legislation applicable in Scotland and Northern Ireland. If they do so they have the power to take, without consent, that person's DNA and fingerprints, in the exact same way as they would for any other arrestee[173].

ii The police may arrest a person reasonably suspected to be a terrorist under powers set out in section 41 of the Terrorism Act 2000 (TACT). The police have the power to take, without consent, that person's DNA and fingerprints[174].

iii Schedule 7 of TACT also gives the police and others broad powers to stop, search and detain individuals at ports, airports and international rail stations, including (but not limited to) where they suspect the person has been concerned in the commission, preparation or instigation of acts of terrorism[175]. DNA and fingerprints can be taken from those detained under Schedule 7 either with or without consent, depending on the circumstances, according to powers set out in Schedule 8 of the same Act[176] (see also paragraph 224 below).

iv The police may also receive DNA profiles and fingerprints from overseas partners or other agencies.

223. A significant proportion of the biometrics of which I have oversight are taken when someone is stopped and detained under Schedule 7 powers. These stops are made by police officers specifically trained and accredited to exercise Schedule 7 powers and may be made for a number of reasons, including the behaviour of the individual, a referral from a Border Force officer, the individual being on a 'watchlist' or a specific request being made by the Security Service to stop and question the person. The stops (and subsequent detentions) made at the behest of the Security Service are of interest as often the later decision to retain biometrics for reasons of national security will also be heavily influenced by the view of the Security Service.

171 See also Appendix C.
172 PACE section 24.
173 See also Chapter 3, Table 1.
174 http://www.legislation.gov.uk/ukpga/2000/11/schedule/8
175 As defined in TACT section 40.
176 http://www.legislation.gov.uk/ukpga/2000/11/schedule/8

I do not, however, have oversight of the Security Service so am restricted in the information that is available to me about what is known about these individuals (see also paragraph 258 below).

224. Biometrics are not always taken when an individual is detained under Schedule 7 powers and there is guidance for officers to assist them in deciding whether to take biometrics, but there has been a push in recent years to take more biometrics from detainees as it was felt that officers were making insufficient use of these powers. A DNA sample and fingerprints may be taken from a detained person at a port only if the individual gives their consent in writing or has been previously convicted of a recordable offence[177]. If the individual does not consent in writing and they do not have a relevant previous conviction, fingerprints and DNA may also be taken at a police station under the authority of a superintendent or higher-ranking police officer[178] for designated specific reasons[179].

BIOMETRICS RETAINED FOR NATIONAL SECURITY PURPOSES

Biometrics taken or received under the powers set out above may be retained according to the ordinary regime for the retention and use of DNA and fingerprints explained in the previous chapter of this Report, depending on the type of offence for which a person has been arrested and whether the person has been charged or convicted of that offence. There are, additionally, automatic initial retention periods that are lawfully permitted for biometrics taken or received under the specific powers set out above. The current initial retention periods are set out in Appendix C of this report although it must also be noted that the Counter-Terrorism and Border Security Act 2019 (CTBS Act) made some changes to these retention periods. The biometric provisions of that Act have not been enacted at the time of writing but may well have been by the time the Secretary of State lays this Report before Parliament. This is explained in more detail at paragraphs 230 to 237 below.

The Protection of Freedoms Act 2012 (PoFA) sets out additional 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 (i.e. none of the aforementioned retention periods apply or the initial statutory retention period will shortly expire, and the person is still of national security interest).

A responsible Chief Officer or Chief Constable[180] 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.

An NSD must be in writing and lasts for a maximum of two years beginning with the date it is made.[181] An NSD may be renewed for a further period of two years and can be considered for renewal on any number of further occasions.

177 There is a further question here about the nature of the 'consent' given that the person is in detention, is being questioned and may well be unfamiliar with their rights and/or just keen to be released and on their way.
178 Similar provisions in Scotland are set out in the Criminal Procedure (Scotland) Act 1995.
179 TACT 2000, Schedule 8, paragraph 10.
180 (i.e. the Chief Officer or Chief Constable of the force or authority that 'owns' the biometric records at issue).
181 The statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different (see further Appendix C). Further, this 2 year retention period will be extended to 5 years once the biometric provisions of the CTBS Act come into force.

225. My job as regards National Security Determinations (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.

226. 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.[182] 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.

227. 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[183] and have access to the various police biometrics databases.

BIOMETRIC DATABASES FOR COUNTER TERRORISM

228. The counter-terrorism (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 (SOFS). The CT Fingerprint Database is a separate and secure database within IDENT1 for CT related fingerprints and crime scene fingermarks. The biometrics of individuals who are arrested, charged and/or convicted and who are of national security interest will be held on the National DNA Database (NDNAD) and national fingerprint collection on IDENT1 in the usual way, according to the usual PoFA retention regime. They may also be held on the CT biometric databases. DNA profiles and fingerprints held due to the making of an NSD will be held on the CT biometric databases only.

229. All DNA profiles loaded to the NDNAD can be and are 'washed through' against the CT DNA database. All new tenprint fingerprint sets loaded to IDENT1 are automatically 'washed through' the CT Fingerprint Database. There is a similar arrangement in place that allows the automatic searching of crime scene fingermarks on the CT fingerprint database against the immigration and asylum fingerprint database (IABS). There are restrictions in place to ensure that only those with the relevant clearance, working in CT policing, are able to view the results of such searches.

LEGISLATIVE CHANGES AFFECTING NSDS

230. Following the terrorist attacks that took place in the UK in 2017 the then 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 Act makes some changes to the police retention and use of biometrics for counter-terrorism purposes. The biometric provisions have not yet come into force as the Home Office is required to take Statutory Guidance through Parliament that sets out in more detail the rules and

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

practical requirements for the making of NSDs. The police also needed some time to make the necessary changes to their processes and IT systems. It was initially planned that the Guidance would be progressed, and the biometric provisions would come into force, around November 2019 but the political upheaval in the latter part of the year and subsequent general election caused this to be delayed. It is now expected that the provisions will come into force in the spring of 2020, or in any event after this report has been completed and presented to the Home Secretary.

231. 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. The new Act does say that an NSD can be made for a maximum of five years and I have made clear to the Counter-Terrorism Command and the Home Office that I expect NSDs to be made only for a period of time that can be shown to be necessary and proportionate. The new (currently draft) Statutory Guidance makes it very clear that there should be a mechanism in place to allow for NSDs to be made for time periods of less than five years and that whatever time period is chosen there must be sufficient justification for this.

232. 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. However, I am only aware of a very small number of NSDs that were cancelled before the two year retention was completed[184]. 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 to review them at appropriate intervals before the maximum period is completed.

233. 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 powers in 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 standard power of arrest in PACE.[185] 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.

234. 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

184 For example I am aware one case during 2019 where the subject died during the two year period, resulting in the NSD being closed several months before expiry.

185 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.

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. 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.

235. There remains a small risk that the police will continue to want to make pre-emptive NSDs in relation to biometrics taken when an individual is being investigated for non-terrorism related offences or has been charged but not convicted for non-terrorism related/non-qualifying offences but where the individual is still considered to be a threat to national security. In these cases there is no automatic retention period if an individual is arrested (or for a non-qualifying offence charged but not convicted) but subsequently no action is taken against them. In order to mitigate this risk, as I understand it there is a provision in the (draft) Statutory Guidance on the making of NSDs which allows an additional period of up to six months after an investigation has ended for the police to complete all of the processes needed to make an NSD. This needs to be kept under careful review both to ensure that no further pre-emptive NSDs are made and because the police still need to put in place practical measures to ensure that biometrics are not destroyed in error at the end of such investigations.

236. 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 judgements or of the wider national security context. I commented in previous reports 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 my successor will need to be alert to such a risk in carrying out their obligation to review all NSDs.

237. 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

238. In previous Reports I have commented 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 had 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. I was pleased to report last year, however, that I have found both the Counter-Terrorism Command and PSNI to be making every effort to be compliant with the provisions of PoFA and that this has largely now been achieved.

239. Further, I am particularly grateful for the level of engagement with myself and my Office that has been evident throughout 2019 and for the helpful and proactive way that both the Counter-Terrorism Command and PSNI have responded to my interventions and requests.

240. During 2018 FIND-SB added the CT biometric databases to their governance, where they are dealt with in the same way as other police DNA and fingerprint database holdings. This has proved during 2019 to be a significant step in improving the governance of the CT databases and is essential as the new HOB data platforms come into use. Also during 2018 the Counter-Terrorism Command introduced direct reporting by the PoFA CT Programme Board to the National Security Biometrics Board, which is chaired by the Commander of the MPS Counter-Terrorism Command. It was agreed that this governance structure would form part of my oversight, including attendance by myself or a member of my staff at each of these Boards. This is a higher level of accountability than applied in the past and, having now been in place for over a year, appears to be effective in ensuring that robust governance is in place and that the problems of the past are not repeated.

SECTION 18 COUNTER-TERRORISM ACT 2008

241. I explained the year before last 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. I reported last year that this situation had been resolved and the deletion of the unlawful holding was in progress. Unfortunately, I was then informed that 275,000 fingerprint records are being held unlawfully (albeit in an unsearchable format) due to administrative issues and new governance put in place to avoid the inadvertent deletion of legally held material. The police and Home Office assured me over a year ago that they were working to rectify this as soon as possible. Unfortunately, at the time of writing there are still 298,572 tenprint fingerprint records and 1,290 crime scene fingermarks awaiting ‘bulk

deletion'. These records are not being held in a searchable format but are nevertheless being held unlawfully.

MOD SEARCHING INTO THE POLICE NATIONAL FINGERPRINT DATABASE

242. 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, as explained above, a separate CT 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, 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.

243. I reported both last year and the year before that the MoD want to check whether fingerprints taken or found during military operations abroad match to persons known to the UK police or immigration authorities or match crime scene fingerprints held by the police. In order to perform these checks a search must be made against 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[186].

244. 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.[187] 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.

245. 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 during 2018 to the Permanent Secretary of the MoD seeking clarification on this issue. Over the last two and a half years 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.

246. 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 Chiefs' Council (NPCC) represents the collective interest of these Chief Officers. 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. They did this initially over a year ago and counsel for the police, providing the advice, did not identify any lawful basis for the status quo. I reported in my 2018 Annual

186 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.

187 As amended by PoFA.

Report that as a result of this advice two possible solutions were proposed and these were being evaluated and developed by the police, MoD and Home Office. It seemed at that time that matters were being progressed at pace and that the NPCC would be making a decision on the matter imminently.

247. In June 2019 I was disappointed to report, in an Addendum to my 2018 Report, that there had been no discernible further progress despite the clear urgency, that the options did not appear to have been evaluated and developed further by the parties and that a decision had not yet been taken by the NPCC.

248. All parties agree that whilst the searching is in the national interest, a clear lawful basis for doing so, with clear governance and oversight arrangements and appropriate scientific standards in place needs to be found and implemented urgently. At the time of writing the matter remains unresolved, despite the considerable efforts of the Chair of the FIND Strategy Board and others to find a resolution. The NPCC are currently awaiting further legal advice from counsel, having had additional input from the police, MoD and Home Office. I am assured that once this further legal advice is finalised that the NPCC will be asked to consider whether it will allow these searches to continue and, if so, through what mechanism and on what basis. I am extremely disappointed at the time it has taken to reach this point and at the seeming determination of some of the parties to repeatedly derail efforts to bring the matter to a swift resolution.

USE OF THE CT DATABASES

249. 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 2018 was some 11,850 and as at 31 December 2019 was some 8,666[188]. Those latter figures encompass both new additions to the databases since 31 October 2013 and deletions from those databases after that date. Of the individuals whose biometric records were being held by the police on those databases as at 31 December 2019 some 2,018 (i.e. about 23%) had never been convicted of a recordable offence.

188 There appears to be a considerable discrepancy between this and the figure for 2018 which is currently being investigated by SOFS.

TABLE 19: Holdings of biometric material on the CT Databases (year ending 31 December 2019)

		2018	2019
DNA	**DNA**	8,109	9,376
	Of which unconvicted	1,406 (17%)	2,138 (23%)
Fingerprints	**Fingerprints**	11,168	11,741
	Of which unconvicted	1,877 (17%)	2,281 (19%)
Totals	**Total holdings of material**	19,277	21,117
	Of which unconvicted	3,283 (17%)	4,419 (21%)
	Individuals on databases[189]	11,850	8,666[190]
	Of which unconvicted[191]	1,994 (17%)	2,018 (23%)

Source: SOFS

THE NSD PROCESS

250. As explained above, deciding whether an NSD should be approved is a matter for a Chief Officer of police.[192]

251. 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 230 to 237 above).

252. 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[193] as additional supporting information for the NSD decision. After recent terrorist incidents and the report by David Anderson QC[194] 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 continue to engage with the Service on this matter as where, as they are in some cases, the codes are instrumental to the Chief Officers' decision,

189 taking into account those with DNA and fingerprints held.
190 There appears to be a considerable discrepancy between this and the figure for 2018 which is currently being investigated by SOFS.
191 taking into account those with DNA and fingerprints held
192 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.
193 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.
194 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

and my subsequent oversight of that decision, it is essential that sufficient information is available for properly informed decisions to be taken.

253. 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.[195]

254. 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. I also receive copies of any applications that were refused by Chief Officers so that I can oversee the entirety of the process.

255. 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 decline when the number of Chief Officers who can agree to NSDs is reduced.

256. During 2019 the cases of approximately 1,374 individuals who had never been convicted of a recordable offence but whose biometric records were nonetheless being retained on the national CT databases were reviewed by the Counter-Terrorism Command or PSNI for NSD purposes.[196]

257. As can be seen in Table 20, 398 NSDs were made by the Counter-Terrorism Command and PSNI during 2019. This is a decrease of 20% compared to last year, which can be accounted for by the smaller number of renewal NSDs this year. This does mean however (given that NSDs are currently made for two years) that there is expected to be a bulge in renewal cases during 2020. I supported 367 of the NSDs made in 2019 and I raised challenges in 26 of the cases I examined. In 6 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.[197]

195 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) A new version of this Guidance will be taken through Parliament shorty as a result of the changes made by the CTBS Act.

196 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 2019 reporting year.

197 Some NSDs made in late 2019 will have been considered by the Commissioner in early 2020 are not included in this figure.

TABLE 20: NSD decisions (year ending 31st December 2019)

	2018	2019
Total possible NSDs applications processed	**1,480**	**1,374**
Renewal NSDs considered	448	262
New NSDs considered	1,032	1,112
NSDs approved by Chief Officer	**497**	**398**
Renewals	228	117
New NSDs	269	281
NSDs declined by Chief Officer	**32**	**25**
Renewals	15	7
New NSDs	17	18
NSDs supported by Commissioner	468[198]	367[199]
NSDs challenged or further information sought	55	26
Destruction ordered by Commissioner	11	6

Source: SO15 and PSNI

258. 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 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 are introducing 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

259. I am required to keep under review the process of making NSDs and the use to which retained material is subsequently put. In previous years I have reported 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. During 2018 the Counter-Terrorism Command and the MPS Secure Operations Forensic Services (SOFS) were able to provide me with some more data and further narrative about the use to which some of the NSD retained material had been put. However, the detail in the reporting continued to be very restrictive because of lack of resourcing.

260. During 2019 the Counter-Terrorism Command and the MPS Secure Operations Forensic Services (SOFS) have provided me with greater detail than they have ever been able to

198 Some NSDs made in late 2018 will have been considered by the Commissioner in early 2019.
199 Some NSDs made in late 2019 will have been considered by the Commissioner in early 2020.

previously. This is, however, still limited until a bespoke case management system to manage such cases is brought into use. As can be seen in Table 21 below the majority of biometric matches against NSDs came about from arrests and further Schedule 7 stops. This in itself may be beneficial to national security as it evidences the increased capability to identify subjects of national security interest entering and leaving the UK using biometrics, regardless of what identity they may be using.

TABLE 21: Matches with NSD retained material (year ending 31 December 2019)

Type of biometric match	Number of matches	
	2018	2019
Fingerprint Crime Stain to Ten Prints	1	4
Ten print (Arrestee/Sched 7 etc) to Ten Prints	72	106
DNA Crime Stain to DNA Reference Profile	3	1
DNA Reference Profile to DNA Reference Profile	32	20
DNA Arrestee to DNA Reference Profile[200]	9	8

Source: SOFS and SO15

261. A dip sample has also been undertaken by the Counter-Terrorism Commend across 23 cases in this reporting period, where a newly taken biometric matched to NSD retained material (this equates to 16.5% of all matches). Some in depth case studies have also been provided to me. Of particular note are the following:

i In one case a DNA profile held under an NSD was matched to an unidentified crime scene stain.

ii In four cases fingerprints held under an NSD were matched to an unidentified fingerprint taken from a crime scene.

iii Of the Schedule 7 matches to biometrics held under an NSD three related to individuals suspected of travelling to take part in the Syria/Iraq conflicts.

iv In many cases, a match to biometrics held under an NSD provided intelligence to the police and others about overseas and other activities by the individual.

v In several cases, the NSD held biometric match provided potential evidence of offences, including terrorist offences and fraud.

vi In several cases, the match to material held under an NSD resulted in a visa application being refused due to the subject's involvement in overseas terrorist activities and the individual therefore being prevented from entering the UK.

vii In one case, the match to biometric material held under an NSD resulted in the subject being detained and being subject to deportation from the UK due to their involvement with a proscribed organisation.

262. It is also possible to give some additional context to the above by highlighting the wider work done by the police using biometrics linked to individuals of national security interest, not just those held under NSDs. For example, during 2019 the police received over 800 'biometric notifications' against the CT fingerprint database in relation to asylum applications, visa

200 These are matches to material held under an NSD.

applications and applications made for biometric residence permits. Having looked into these potential matches the police found that nine individuals who had applied for asylum, 22 individuals who had applied for a biometric residence permit and 34 individuals who had applied for a visa had links to CT related intelligence, with subsequent appropriate action taken, including preventing individuals from entering the UK.

263. The Counter-Terrorism Command also manage the intelligence response to any matches made under the Prüm exchanges (see also Chapter 5) which may be linked to CT investigations. To date there have been 65 DNA matches which may be of national security interest.

264. I appreciate the work done by the Counter-Terrorism Command to provide me with this data, dip sample and additional information. However, as routine tracking of every NSD case is not possible with the current case management system I am still not providing the Home Secretary with the level of detailed information about 'the use to which the biometric material is put' which I believe is required under PoFA. I hope that the new case management system that they are introducing 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.

NSDS IN NORTHERN IRELAND

265. 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.

266. 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 transitional period in Northern Ireland for a further two years, until 31 October 2018[201] and was repeated again in 2018, until 31 October 2020.[202] This Order applies only to Northern Ireland biometric material taken under counter-terrorism powers before 31 October 2013 ("pre-commencement material") and because Legacy records may be needed as part of that historical cases review process, it *"seeks to ensure that the timing of commencement of the destruction provisions in relation to biometric material taken under counter-terrorism powers in Northern Ireland allows for political agreement on legacy investigations to be reached"*.[203]

267. The upshot of this amendment is that national security pre-commencement material in Northern Ireland is not subject to the relevant destruction and retention provisions for pre-commencement material until 31 October 2020. If a further such a Statutory Instrument is passed by Parliament, then this period could be extended. If not, PSNI must either consider legacy material for an NSD or delete it by that date. The government has reaffirmed its commitment to introducing legislation addressing the legacy of the past, as set out in 'New Decade, New Approach'; and on 18 March 2020 the government set out the way forward on this – announcing the start of an intensive engagement phase on proposals prior to bringing forward legislation. We will remain in close contact with the Secretary of State and his officials as this work is taken forward.

201 http://www.legislation.gov.uk/uksi/2016/682/contents/made
202 http://www.legislation.gov.uk/uksi/2018/657/contents/made
203 http://www.publications.parliament.uk/pa/ld201617/ldselect/ldsecleg/25/2504.htm

268. 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. I and my Office have visited PSNI twice during 2019 and have found PSNI to be fully compliant in relation to material taken under counter-terrorism powers since the commencement of PoFA. It must be noted, however, that NSDs made by PSNI represent only a small proportion of the total number of national security holdings as they are only made in relation to new biometric material, due to the legacy arrangements outlined above[204].

DATA LOSSES

269. 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 2019 it appears that the majority of these issues have now been resolved. As can be seen in Table 22 below, 144 biometrics were lost during 2018 but during 2019 only four were lost. These were all due to administrative errors. I am informed by the Counter-Terrorism Command that of those four losses of biometric material only one would have been considered for retention under an NSD. Necessary steps have been taken to assess the necessity and proportionality of re-acquiring the lost biometric material. The new case management system being implemented by the Counter-Terrorism Command should further mitigate the risk of these type of errors in future.

TABLE 22: Losses of biometric material of potential CT interest (year ending 31 December 2019)

Reason for loss of biometric data	Number of losses of biometric material	
	2018	2019
Administrative error by SO15/SOFS	104	4
Case not reviewed by Chief Officer within statutory time limit	8	0
Case not progressed within statutory time limit	8	0
Taking of material not notified to SOFS	24	0

Source: SO15

FUTURE GOVERNANCE OF BIOMETRICS FOR NATIONAL SECURITY

270. As is alluded to in this chapter the police Counter-Terrorism Command are working increasingly closely with the MoD and the Security Service. Representatives of both these bodies attend the NSBB, which is sensible given that this reflects current practice. Slightly at odds with this, however, is the current legislative regime as set out in PoFA, which at the time it was drafted essentially envisaged the police being solely responsible for the collection, retention and use of DNA and fingerprints for domestic national security purposes. Furthermore, facial image collection, retention and use for the purposes of national security is now routine but is not governed by PoFA. This raises an important question, particularly in light of the government's manifesto commitment to legislate in this area (see also Chapter 2). For the future – does

204 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.

Parliament wish to re-assert the primacy of the police in domestic national security capture, retention and use of biometrics or instead does it want to legislate to cover the roles of the police, the Security Service and the MoD in their use of biometrics for domestic national security? The choice has implications for how far the Counter-Terrorism Command remain closely linked to the rest of policing or become rather separate and more closely linked to the Security Service and the MoD. It also has implications for how the future governance of the use of biometrics for national security should be structured.

5. INTERNATIONAL EXCHANGES OF BIOMETRIC MATERIAL

271. 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[205] states that:

> *"The Biometric Commissioner will dip sample cases in which a person's DNA and/or fingerprints material has/have been exported from the UK to make sure that this has been done appropriately."*

272. It should be noted that many of the biometric exchange mechanisms referred to in this chapter are EU mechanisms. Whether the UK will continue to have access to these mechanisms once the Brexit transition period has ended and the extent to which the involvement of the UK in EU biometric exchange mechanisms will form part of any exit deal with the EU is unclear.

POLICY QUESTIONS

273. The international exchange of DNA profiles and associated demographic information is governed by the Home Office *International DNA and Fingerprint Exchange Policy for the United Kingdom*[206]. 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 previously no equivalent Home Office policy for the international exchange of fingerprints (the former policy covered only DNA) and this governance deficit left those agencies responsible for the international exchange of such data to operate without a national government policy steer.

274. 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.

275. FIND-SB has now produced this new policy. A key issue in discussions about that new policy 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[207] 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 have said repeatedly that I am not convinced that this distinction can be easily made nor why it has the implication claimed. The new FIND-SB policy 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.

205 https://www.gov.uk/government/publications/international-dna-and-fingerprint-exchange-policy-for-the-uk
206 Previously the *International DNA Exchange Policy for the United Kingdom*.
207 DNA samples are very rarely exchanged.

THE ROLE OF THE NCA, ACRO, THE COUNTER-TERRORISM COMMAND AND THE ICCC

276. The NCA has a coordination and liaison function as regards the exchange of biometric material between the UK and foreign/international law enforcement agencies. It deals with international fugitives, 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.

277. 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.

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

279. The Counter-Terrorism Command also exchanges biometric information, as well as intelligence, with foreign powers[208]. For example, they can share biometrically enabled watch lists with partner countries. They also receive biometrics (usually in an anonymised form), which may then be retained on the UK CT biometric databases, from overseas partners. This process allows the sharing of fingerprint and DNA data with selected countries with whom specific agreements have been made for sharing, in order to secure borders, and prevent and detect terrorist activity.

280. The International Crime Coordination Centre (ICCC) is a national police unit that was initially established to provide continuity for UK law enforcement following the UK's withdrawal from the EU. The unit provides a range of advice, support and guidance on policing measures and tools available to tackle all forms of international criminality. They are also working closely with government and other operational partners to identify and ensure that a range of contingency measures are in place should the UK lose access to EU based law enforcement and exchange mechanisms.

281. In addition to their role in contingency planning the ICCC are currently working to establish a national police training programme, to ensure that all police officers and forces are aware of when and how to access, and utilise fully, appropriate international exchange mechanisms. I welcome this, whether the UK maintains access to existing EU exchange mechanisms or not, as even those currently available have to date been, in my view, underutilised. Given the global nature of the world in which we live and the increasingly international element to criminality this appears to me to be both vital and overdue in UK law enforcement.

208 Particularly with EU partners.

EXCHANGE OF FINGERPRINTS AND DNA FOR INTELLIGENCE PURPOSES

282. 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.

i. DNA samples

283. DNA samples are only exchanged in very rare situations where the subject consents. During 2019 no DNA samples were exchanged with other countries.

ii. DNA profiles

284. DNA profiles are sometimes exchanged with other 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 23 below provides the figures for inbound and outbound DNA Requests.

285. There are 4 types of DNA profile enquiry that are dealt with by the NCA.[209]

- *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.
- *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.
- *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.
- *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'.[210] 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*".

209 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.

210 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.

TABLE 23: DNA Profile Enquiries (year ending 31 December 2019)

	Outbound from UK			Inbound to UK		
DNA Type	**Total**	**Searches concluded**	**Positive/ potential Match**	**Total**	**Searches concluded**	**Positive/ potential Match**
DNA samples	0	0	0	0	0	0
DNA subject profiles	19	16	1	53	31	1
Missing persons	12	9	1	19	16	0
DNA crime scene profiles	27	25	1	25	22	5
Unidentified bodies	1	0	0	22	19	4

Source: NCA

iii. Fingerprints and finger-marks

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

- *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.
- *Inbound fingerprints:* Inbound requests occur when a foreign country sends fingerprints to the UK, for example to confirm identity.
- *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.
- *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.[211]

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

TABLE 24: Inbound and Outbound Fingerprint Requests (year ending 31 December 2019)

	Outbound from UK			Inbound to UK		
Fingerprint Type	Total	Searches concluded	Positive/ potential Match	Total	Searches concluded	Positive/ potential Match
Ten Print Sets	565	16	27	1,067	386	99
Crime Scene Fingermarks	21	0	0	160	24	**1**

Source: NCA[212]

iv. Dip sampling

287. In previous years I have undertaken an annual dip sampling exercise, during which I have visited the offices of the NCA and dip-sampled cases where an international biometric exchange took place, some of which were exchanges of DNA and some of which were fingerprint exchanges. This year I have not done so due to the political uncertainty throughout the year about when and on what basis the UK was to leave the EU and the subsequent uncertainty around the continuation of international biometric exchanges, but I assume my successor will do so once there is more clarity on this matter. I am also aware that there has been considerable pressure on the International Crime Bureau (UKICB) at the NCA in terms of getting the Prüm DNA exchange process up and running and then dealing with the subsequent matches, so I had not wished to put them under any more pressure in the short term. My Office has though maintained regular contact with the NCA, met with UKICB staff, had sight of biometric exchange data and visited the NCA in relation more generally to their use of DNA and fingerprints during 2019. A full audit of the Prüm DNA exchanges is also due to be undertaken by my Office, together with the ICO, in early spring (see also paragraphs 307 to 314 below).

EUROPEAN ARREST WARRANTS

288. 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).

289. 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[213] and is responsible for recording all requests received through the Sirene system.

212 Here is some uncertainty as to whether these figures are correct as I have seen several different connotations, depending on the source and counting methodology used.

213 '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).

290. 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.

TABLE 25: EAW Requests by fiscal year (2014/15 – 2019/20)[214]

	2014/15	2015/16	2016/17	2017/18	2018/19
Requests from the UK	223	241	345	296	Data not available
Requests into the UK	12,134	14,279	16,598	17,256	Data not available

Source: NCA

291. Table 25 gives a yearly comparison of the number of EAWs issued since 2014, as published in the NCA's own data however the data for 2018/19 does not appear to have been published by the NCA to date. Nevertheless, a Home Office impact assessment states that *"15,540 'requests'[215] were made under the EAW process in 2018/19. In that same year, 1,412 arrests were related to EAWs, and 919 to surrenders"*[216]. 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.[217]

292. Notwithstanding the missing/unclear figures, the above data illustrates clearly the utility of the EAW system over a number of years.

293. The current UK government position is that *"the UK is not seeking to participate in the European Arrest Warrant as part of the future relationship. The agreement should instead provide for fast-track extradition arrangements, based on the EU's Surrender Agreement with Norway and Iceland which came into force in 2019, but with appropriate further safeguards for individuals beyond those in the European Arrest Warrant"*[218]. However, the Home Affairs Select Committee has suggested that the Home Office is "overly-optimistic" about the ease with which replacement arrangements can be negotiated. If no new agreement is reached the UK will fall back on previous arrangements. These are contained in a 1957 Council of Europe Convention on Extradition, which will require amendments to domestic legislation. The UK will also be reliant on other Member States making equivalent amendments because some have repealed legislation that gave effect to the Convention since the EAW. It should be noted that prior to the implementation of the EAW, the UK extradited fewer than 60 people each year[219].

294. If the present ease of extraditing accused persons between the UK and the EU is to continue it will need a new arrangement with very similar capabilities to the EAW system. If no such new arrangement comes into being then we will be forced back onto the Council of

214 See https://nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/fugitives-and-international-crime/european-arrest-warrants
215 It is unclear whether this means requests into or out of the UK, or both.
216 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/841191/Impact_Assessment.pdf
217 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.
218 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868874/The_Future_Relationship_with_the_EU.pdf
219 https://commonslibrary.parliament.uk/home-affairs/crime/brexit-next-steps-the-european-arrest-warrant/v

Europe mechanism which, in previous experience, will be much slower and less productive than the EAW.

EXCHANGES OF CONVICTION INFORMATION

295. ACRO exchanges criminal conviction data with the other 27 EU member states under Framework Decision 2009/315/JHA.

296. When UK citizens are convicted of offences abroad there is a legal requirement for their convictions to be notified to the relevant UK authorities.[220] Likewise, when EU citizens are convicted of offences in the UK there is a legal requirement for the UK authorities to inform the authorities in their home country. This is done via the European Criminal Records Information Exchange System (ECRIS), following the 'notifications' process set out below. The UK or EU may also 'request' conviction information where the national of another EU country is subject to criminal proceedings, to find out whether they have convictions in their home country.

a. Exchanges of fingerprints in the context of conviction information

297. Exchanges of the fingerprints of EU and UK nationals take place in response to 'Requests' or 'Notifications'.

- A 'Notification' of conviction information is sent out by ACRO when a national of another member state is convicted in the UK. That Notification is sent to the country of nationality and may be accompanied by the subject's fingerprints. If so, those fingerprints will also be sent to Interpol.
- Notifications are received by ACRO from other member states whenever a UK national is convicted in another EU member state. The relevant conviction information is loaded to the PNC and, when fingerprints are received, they are loaded to IDENT1.
- A 'Request Out' is made when a national of another member state is subject to criminal proceedings in the UK. The request is sent to the country of nationality and seeks information about the subject's convictions (if any) in that state. Sometimes that request will be accompanied by the subject's fingerprints.
- A 'Request In' may be received by ACRO from another EU member state when a UK national is subject to criminal proceedings in that state. The request seeks information about the subject's convictions (if any) in the UK and will sometimes be accompanied by the subject's fingerprints. These fingerprints are used to carry out a 'hit/no hit' search on IDENT1.

298. 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.

299. Table 26 below provides comparative figures in relation to EU and non-EU exchange requests[221].

220 There is no such legal requirement for non-EU countries.
221 The data for this year has been recorded using a different methodology to previous years so these are not directly comparable.

TABLE 26: Fingerprint Exchanges[222] (year ending 31 December 2019)

	EU Exchanges	Non-EU Exchanges
Requests in	349	1,369
Requests out	13,965	18,609
Notifications in	34	50
Notifications out	16,632	17,258

Source: ACRO Criminal Records Office

300. It unfortunately emerged in early 2020 after reports from several news outlets that ACRO had not received details of approximately of 75,000 convictions of foreign criminals and therefore was unable to pass on these convictions to their home EU countries[223]. This appears to have been caused by a technical problem with reports automatically produced from the PNC.

301. In any event, it is clear from the above figures that a large amount of conviction data and fingerprint data is shared between the UK and EU, in particular through the ECRIS system. It would therefore appear vital that the UK maintains access to these EU exchange systems or that an alternative system, with the same capability to share conviction data and associated biometrics with other countries in Europe, with a legal compulsion for this to be done in some cases, is established before the end of the transition period.

b. Loading non UK convictions onto the PNC

302. Unless and until a non UK conviction has been recorded on the PNC, it is impossible to load to the national databases any DNA profile or fingerprints which have been taken in reliance on that conviction. Notably,

- there are strict limitations on the uses to which the UK can properly put conviction information about (non-UK) EU nationals which it obtains from other EU member states;
- it is only in relatively rare circumstances that the foreign convictions of such EU nationals can properly be recorded on the PNC;
- those circumstances are in effect limited to cases where the recording of those convictions on the PNC is reasonably necessary to prevent "*an immediate and serious threat to public security*"; and
- convictions will only be treated as being of that type if they are for offences that fall within the scope of a list of serious offences which has been approved by the Home Secretary.[224]

303. 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.[225]

---

222 These figures include all requests/notifications accompanied by fingerprints, whether to/from Interpol or directly to/from the country concerned. In some cases this may count as two exchanges relating to the same individual/conviction, with one set of fingerprints sent to the home country and another sent to Interpol.

223 https://www.theguardian.com/uk-news/2020/jan/14/revealed-uk-concealed-failure-to-alert-eu-over-75000-criminal-convictions#maincontent

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

225 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,

304. 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.

305. 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.

c. UK nationals who have offended abroad

306. No 'loading' difficulties arise as regards the convictions of UK nationals who have offended abroad 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.[226] 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.

PRÜM

307. The Prüm Council Decisions of 2008[227] allow for the reciprocal searching of DNA and fingerprint databases within the EU on an anonymised 'hit/no hit' basis and also the exchange of vehicle registration data. The UK initially opted out of the Prüm exchanges. However, in December 2015[228] 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 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.

308. Both I and the Information Commissioner have a role in overseeing and auditing the Prüm exchanges. Together with the ICO my Office have carried out a scoping visit to the Metropolitan Police Service (MPS) to look in more detail at how the exchanges are being carried out and it is intended that a full audit will be undertaken during spring 2020. Subsequent to that visit I will agree with my colleague, the Information Commissioner, how we should exercise our oversight function in the future, assuming, of course, that we remain part of the Prüm exchanges. The FIND Strategy Board will also have a role in overseeing the exchanges.

United Arab Emirates, United States of America, Sovereign Base Area of Cyprus.

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

227 2008/615/JHA and 2008/616/JHA

228 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.

309. The Prüm DNA exchanges to/from the UK began to operate in July 2019 and the UK is now connected to Austria, Germany, France, the Netherlands, Spain, Romania, Poland and the Czech Republic. Prüm allows the UK to search an anonymised version of Member States' DNA databases. These searches produce an initial 'hit'/'no-hit' response of an identified matching DNA profile. Step 1, carried out by the MPS, is the initial 'hit'/'no-hit' response.

TABLE 27: Prüm Step 1 exchanges (year ending 31 December 2019)

	Hits for the UK	Hits for EU Member States
Legacy hits	11,554	40,544
Business as usual hits	882	

Source: Metropolitan Police Service[229]

310. Following scientific verification that a 'hit' is a true one, the UK can request further information. This is Step 2 and is the point at which demographic data and crime investigation details may be exchanged – once a match has been verified.

311. Outbound Step 2 requests refer to requests made by the UK where there has been a match of UK data against Member States' systems, the match has been verified, and a request is made by the NCA to the relevant Member State for the demographic information or crime investigation details associated with the match[230]. Inbound Step 2 requests refer to requests where there is a verified match against UK systems for a Member State and that Member States carries out a request to the NCA[231] for the demographic information associated with the match[232].

229 These are unverified hits that need to be verified by operational partners (in the UK and with the EU Member States) to eliminate false positives.
230 All outbound requests are prioritised according to seriousness, urgency and capacity to respond.
231 This match is then scientifically validated by the UK before any request is processed.
232 All inbound requests are prioritised according to seriousness, urgency and capacity to respond.

TABLE 28: Prüm Step 2 exchanges (year ending 31 December 2019)

	Outbound from the UK		Inbound to the UK	
	Total	Searches concluded	Total	Searches concluded
Step 2 requests for demographic information	114	84	426	103

Source: NCA[*233]*

312. No exchanges of fingerprints have yet been undertaken under the Prüm mechanism and at the time of writing it is unclear when/if this will be agreed with the EU and, if so, when/if it will start taking place[234].

313. As is clear from the above data the exchanges of DNA profiles and unsolved crime stains that have already taken place under this mechanism have yielded very significant results compared to the other EU exchange mechanisms. Due to the large number of potential matches there is inevitably a delay and a resourcing question around the work that needs to be done to verify the potential matches and the further work that then needs to be done to pursue the leads provided by the matches. For this reason potential matches are prioritised according to the quality of the potential match and seriousness of the alleged offence.

314. I am informed that previously unknown perpetrators of serious offences, including serious violent and sexual offences, have already been identified through the Prüm mechanism and, given the large number of matches that have been made and continue to be made, I expect that this mechanism will continue to be an extremely useful tool for law enforcement in the UK. Whether the UK will be able to remain part of the Prüm mechanism at the end of the transition period remains unknown at the time of writing but there are clearly serious questions to be asked about how such functionality could be replicated were the exchanges through this mechanism to cease.

INTERNATIONAL EXCHANGES LOOKING AHEAD

315. As I write the outcome of negotiations with the EU is unknown. Not all international exchanges depend on EU arrangements and, regardless of the outcome of the negotiations, the UK will remain within broader exchange mechanisms such as Interpol[235]. 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 outcome of the negotiations with the EU.

316. If the outcome of the negotiations is that we lose access to EU exchange mechanisms such as ECRIS, Prüm 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, unless other mechanisms, with similar capabilities, can be agreed upon and established. I welcome the work being done by the ICCC and ACRO to plan for such an eventuality but I

233 This data refers to exchanges that have taken place since Prüm went live in July 2019, between the Member States the UK had connected to during this time (Austria, Germany, France, The Netherlands, Spain). There is not yet a regular reporting cycle for Prüm, however, it is intended that once connections have been made to all the EU Member States a more consistent reporting process will take place.

234 HOB are building the capability for Prüm fingerprint exchanges within IDENT1.

235 See Table 26 for data on these non-EU exchanges

remain deeply concerned about the potential risks for UK law enforcement of the loss of these exchange mechanisms with the countries of the EU.

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[236]

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.

236 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[237] 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.[238]

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 93 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.[239]

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.[240]

- 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'.

237 See section 118 of PACE
238 See (new) section 65B of PACE and section 65 of the Crime and Disorder Act 1998.
239 See section 65A(2) of PACE
240 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

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

Material Retained for the Purposes of National Security

10. Finally, the new regime also allows for the extended retention of DNA profiles and fingerprints on national security grounds if a National Security Determination ('an NSD') is made by the relevant Chief Officer.[241] 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)

11. Where a person without previous convictions is charged with a qualifying offence or where the Biometrics Commissioner accedes to an application under section 63G(2) or (3), by section 63F of PACE[242], 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

12. 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[243].

13. For those persons whose biometrics were taken by police before 03 April 2017, by sections 61(6D), 62(2A) and 63(3E) of PACE[244] 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[245] 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

241 See sections 63M and 63U of PACE as inserted by sections 9 and 17 of PoFA) and Schedule 1 of PoFA.
242 (as inserted by section 3 of PoFA)
243 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.
244 (all inserted by section 3 Crime and Security Act 2010)
245 (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.[246] Whereas a chief officer may only make an application under section 63G(3) if they consider that the retention of the material *"is necessary to assist in the prevention or detection of crime"*, section 63G(2) imposes no express requirement that there be some anticipated public interest in the retention of the material.

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

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

v Although it is provided at sections 63G(5) and (6) that the person to whom the material relates must be informed of any application for extended retention and given the opportunity to make representations against it[247], 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[248]. [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.]

246 These terms are defined at section 63G(10).
247 Further relevant provisions are at sections 63G(7) to (9).
248 There have continued to be some difficulties with this approach during 2019, 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 134 to 136.

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.[249] The Strategy Board endorsed the approach which I had decided to adopt as regards such applications and the detailed Guidance document which it issued in September 2013 (and into which 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 FIND 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.*

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

Relevant Factors

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

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

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

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

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

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

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

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

OBC DOCUMENTS

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[250], the 3 year retention period may be extended for a further 2 years if, following an application by the relevant Chief Officer under section 63F(7), a District Judge so orders. The decision of the District Judge may be appealed to the Crown Court.[251]

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

APPENDIX C

National Security Provisions

STATUTORY BACKGROUND AND GUIDANCE AS TO NSDS

Statutory Background

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

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

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

3. PoFA introduced stricter rules as regards the retention by police forces anywhere in the United Kingdom of biometric material which has been obtained from unconvicted individuals pursuant to TACT, the CTA or the TPIMs Act. The police and other law enforcement authorities may retain DNA profiles and fingerprints for an extended period on national security grounds but they may only do so pursuant to a National Security Determination or 'NSD'.[252]

4. An NSD is a determination made by the responsible Chief Officer or Chief Constable.[253] It must be in writing and, in England, Scotland and Wales, it has effect for a maximum of 2 years beginning with the date it is made. Although the statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different,[254] in practice the same 2-year maximum is applied. An NSD may be renewed before its expiry for a further period of 2 years.[255]

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.

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

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

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

255 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[256]:

   (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.[257] 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[258] as issued can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208290/retention-biometric-data-guidance.pdf.

256 NSDs will also be able to be made under paragraph 46 of Schedule 3 to the CTBS Act once it comes into force.
257 (see footnote 221 above).
258 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."* [259]

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.

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

259 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."*

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.[260]

260 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[261] 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[262]. 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:

261 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)

262 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[263]
Paragraph 20B Terrorism Act 2000 (TACT)	DNA profiles/fingerprints relating to persons detained under s.41 TACT.	3 years[264]
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.

263 The retention period starts from the date the relevant DNA sample/fingerprints were taken unless otherwise stated.
264 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.

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 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

CCS0220195130
ISBN 978-1-5286-2028-4