Annual Report 2020

COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

Fraser Sampson

November 2021

OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

ANNUAL REPORT 2020

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

November 2021

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

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

ISBN 978-1-5286-2890-7
E02669527 11/21

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of Her Majesty's Stationery Office

OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

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

31st August 2021

Dear Home Secretary

Annual Report – 2020

Having been appointed as Commissioner for the Retention and Use of Biometric Material I am required under s.21(1) of the Protection of Freedoms Act 2012 (PoFA) to make a report to you about the carrying out of the Commissioner's functions. My appointment having taken effect from March 2021, this – my first – Annual Report covers a period when the Commissioner's functions were, for the most part, the responsibility of my predecessor.

I am pleased to attach my report for 2020 which will be the seventh annual report of the Commissioner for the Retention and Use of Biometric Material.

Key points in the report include:

1. Compliance with the requirements of the legislation is generally good and I have been impressed with the level of commitment from the police forces and their elected local policing bodies with whom I have engaged, together with that of law enforcement partners.
2. Use of the biometric retention regime established under section 63G of PACE 1984 (as amended by PoFA) varies across police forces, though many of them find it a useful tool to manage risk in certain cases where, although a suspect has not been charged or convicted, it is considered appropriate to retain their biometric material in light of vulnerability factors of the complainant or the chief officer believes that retention is necessary to assist in preventing or detecting crime.
3. The emergency arrangements approved by Parliament under the authority of the Coronavirus Act 2020 empowered you to make regulations allowing the police to extend the statutory deadline for retaining fingerprints and DNA profiles by six months (with the option to extend this for a second occasion by a further six months, up to a maximum of 12 months in total) on grounds of national security in circumstances where there was no other lawful basis to retain these biometrics. This power allowed the police to retain the relevant biometrics without the requirement to carry out a detailed review of the risk posed by an individual and without the need for a chief officer to issue a National Security Determination (NSD) authorising retention. My predecessor was consulted on the provisions at the time and provided a report last September. The second and final set of regulations came into effect on 1 October

2020, expiring on 24 March 2021 and I published a report to inform Parliament of their impact. After meeting with the Metropolitan Police Counter-Terrorism Command (CT Policing) on two occasions to discuss their use of the power, along with their preparations for the transition back to business as usual, I was both reassured by, and impressed with their appreciation that these were short-term transitory provisions born of extraordinary circumstances. I concluded that the regulations have safeguarded biometric information identified as being of national security value, although this necessarily came at the expense of briefly retaining some material later assessed as not warranting further retention on grounds of necessity and proportionality. To that extent, in balancing the lawful interference with individual rights against wider considerations of national security during the extraordinary exigencies arising from the COVID-19 pandemic, the latter were temporarily given limited additional weight in the way clearly foreseen when Parliament passed section 24 of the Act. I saw nothing to indicate that the police applied the provisions in anything other than the manner intended: necessarily, temporarily and proportionately. But for your legislative intervention a considerable number of biometrics held by the police for reasons of national security that would otherwise have been properly retained under an NSD would have been lost. In the event, the second set of regulations allowed some 491 biometrics profiles to be safeguarded and no biometrics which could have properly been considered for retention under the authority of an NSD were lost.

4. The biometric provisions of the Counter-Terrorism and Border Security Act 2019 that were due to come into force when my predecessor last reported to you have improved decision making in relation to National Security Determinations much as he predicted; the creation of a national cadre of trained chief officers will improve this further.

5. It is worth reminding the policing community that, in their work to enable the making and monitoring of National Security Determinations and in the arrangements for handling biometrics required for relevant counter-terrorism functions, the Metropolitan Police Service manages some significant risk on behalf of UK policing; they are to be congratulated for the level of professionalism and purpose with which they approach this critical role.

6. Changes to law and practice referred to in recent annual reports continue to have consequences for the police use of biometrics. Measures introduced to reduce the extent of interference with individuals' human rights and freedoms – such as those affecting bail and encouraging the use of alternatives to arrest – appear to have reduced the number of arrests as intended. However, because the ability of the police to take biometrics is often dependant on the arrest of the individual, the reduction in arrests has produced a correlative reduction in the number of initial speculative searches and of new DNA profiles and fingerprints being added to the national databases. Should this trend continue, the efficacy of the biometrics databases can be expected to attenuate.

7. In his last report my predecessor called for strengthened governance, leadership and reassurance in the arrangements for biometrics and policing. The establishment of a Forensic Science Regulator operating from a firm statutory foundation is a welcome

and important improvement in that regard and I am working with the new incumbent, Gary Pugh, to identify opportunities for bringing additional rigour to the relevant areas of policing practice and performance so far as they affect my functions.

While the legislation empowers you to exclude from publication any part of the report if you are of the opinion that its publication would be contrary to the public interest or prejudicial to national security, I have not included any information which I believe would attract the need for excision and hope you will feel able to lay it before Parliament as submitted.

Yours sincerely,

Fraser Sampson
Commissioner for the Retention and Use of Biometric Material

Foreword

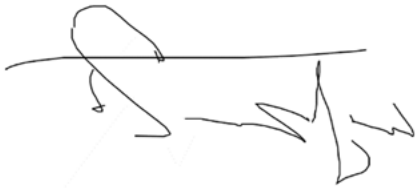
Having been appointed to discharge the statutory functions of both the Biometrics Commissioner and those of the Surveillance Camera Commissioner in March 2021, this – my first – Annual Report covers a period when the respective functions were, for the most part, the responsibility of my two predecessors. As the functions themselves remain discrete within the legislation[1] I have produced two separate annual reports which are published on my website.

I am aware that combining the functions was not uncontentious but the rationale for doing so has found corroboration on many occasions, not least of which was the appearance of the previous Biometrics Commissioner before the Commons Science & Technology Committee in June 2021[2] where he spent some time assisting members with issues arising principally from the use of surveillance cameras.

While the reporting period largely predates my appointment, one particular responsibility that fell to me was reviewing and reporting on the temporary arrangements authorised by Parliament in response to the exigencies of the coronavirus pandemic insofar as they affected National Security Determinations.[3] I reported on this at the relevant time[4] and a summary of that report is included in Chapter 2.

The specific aspects of my role reported on here broadly require me to keep under review the "retention and use" of biometrics in policing in relation to National Security Determinations, counter-terrorism and certain other serious offences where the individual has been arrested but not charged.[5] In doing so, I have followed the structure used by my predecessor.

In both this and my statutory report as Surveillance Camera Commissioner I have highlighted several issues which I believe are relevant to the future of biometrics and surveillance and will return to them in more detail in future annual reports.



Fraser Sampson
August 2021

1 See the Protection of Freedoms Act 2012, Chapters 1 & 2.
2 Wednesday 30 June 2021, oral evidence of the former Biometrics Commissioner, Prof Paul Wiles https://committees.parliament.uk/event/5036/formal-meeting-oral-evidence-session
3 Under the Coronavirus Act 2020, s.24.
4 Report published 29 April 2021 – https://www.gov.uk/government/publications/regulations-made-under-section-24-of-the-coronavirus-act-2020
5 *Loc cit* s.20(2)-(9).

Contents

Foreword iv

1. Biometrics for Policing and Law Enforcement in England and Wales 1

2. Biometrics and National Security 30

3. International exchanges of biometric material 43

Appendix A 54

Appendix B 58

Appendix C 62

List of Acronyms 68

1. Biometrics for Policing and Law Enforcement in England and Wales

1. The Protection of Freedoms Act 2012 (PoFA) established the role of the Commissioner for the Retention and Use of Biometric Material and I am the third person to be appointed to this position. In addition to decision-making powers in relation to applications to retain biometrics[1] and my role to review National Security Determinations approved by chief officers, I am also responsible for keeping under review the retention and use of DNA and fingerprints by the police and reporting annually to the Home Secretary on compliance with the relevant provisions of PoFA. That report is subsequently laid before Parliament. In this chapter I will look at the discharge of those powers and responsibilities by police forces and other law enforcement bodies in England and Wales.[2]

Other independent oversight of biometric use by the police

2. Biometrics provide different degrees of evidential support that any claimed match is true and their quality and evidential use in the criminal justice process is carefully regulated. During 2020, that process was overseen by the Forensic Science Regulator[3] (England & Wales), Dr Gillian Tully, before she stepped down earlier this year. Gary Pugh OBE was appointed as her successor in May 2021 under the provisions of the Forensic Science Regulator Act which will enable Gary to provide guidance and, where necessary, deploy new statutory enforcement powers once they come into force at a date to be decided by the Home Secretary.[4] Fingerprints and DNA are both used and accepted extensively in the criminal justice system in the UK. 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.

3. Facial image matching by the police has attracted significant attention over the past year. While not regulated in the same way as the conventional, established biometrics above, facial image matching may involve the use of public-facing CCTV and surveillance camera systems. The use of such systems by the police is subject to the Surveillance Camera Code of Practice by the Surveillance Camera Commissioner, a role also created by PoFA and previously carried out by Tony Porter. I also have responsibility for this role under my remit as joint Biometrics and Surveillance Camera Commissioner.[5]

4. The Data Protection Act 2018 (DPA) updated data protection laws governing the processing of personal data by the police and others in response to the legislation of the European Union.[6] Part 3 of the DPA reflects and addresses the specific realities of policing and law enforcement functions as recognised by the European legislation[7] and, under that Part, the processing of biometrics is considered to be "sensitive processing".[8] The DPA sets out six data protection principles which apply to law enforcement processing of data. It also details the rights of individuals over their data and places restrictions over those rights, but only where necessary and proportionate to do so. The Information Commissioner's Office headed

1 Made under section 63G of the Police and Criminal Evidence Act 1984 – see paras 78 – 104.
2 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 2 of this report.
3 See http://www.gov.uk/government/organisations/forensic-science-regulator
4 See https://www.legislation.gov.uk/ukpga/2021/14/contents/enacted
5 See https://www.gov.uk/government/news/new-biometrics-and-surveillance-camera-commissioner-appointed
6 Regulation 2016/679 of the European Parliament and of the Council.
7 Regulation 2016/680 often referred to as the 'Law Enforcement Directive'.
8 Data protection Act 2018, Part 3, s. 35(8)(b).

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.[9]

i. Statutory regulation of DNA and fingerprints

5. 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 arrest.[10] Fingerprints are much quicker and cheaper to process and use than DNA and remain a highly reliable form of biometric proof in global use. The way fingerprints are searched and used by the police is different from their use of DNA (see also paragraphs 16 to 20 below). In police custody suites fingerprints are taken from every arrestee on every occasion that they are arrested and are 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).[11]

Retention rules

6. 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;
- if an individual is convicted of a recordable offence their biometrics (DNA profile and/or fingerprints) may be kept 'indefinitely';
- if an individual is charged with, but not convicted of certain more serious offences (called 'qualifying offences'[12]) then their biometrics (DNA profile and/or fingerprints) may be retained for three years; and
- 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.

7. There are, however, a number of exceptions and more detailed qualifications to these general rules relating to things such as 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.

9 https://ico.org.uk/
10 Police and Criminal Evidence Act 1984 (PACE) s. 61 and s. 63.
11 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.
12 See section 65A of PACE. A '*qualifying*' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.

TABLE 1: PoFA Biometric Retention Rules

Convictions

Person	Type of offence	Time period
Adults	Any recordable offence (includes cautions)	Indefinite
Under 18 years	Qualifying offence (includes cautions, warnings and reprimands)	Indefinite
Under 18 years	Minor offences (includes cautions, warnings and reprimands) 1st conviction – sentence under 5 years 1st conviction – sentence over 5 years 2nd conviction	 Length of sentence + 5 years Indefinite Indefinite

Non convictions

Alleged offence	Police action	Time period
All Offences	Retention allowed until the conclusion of the relevant investigation 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	Up to 5 years with an NSD by Chief Officer[13]

Providing assurance on PoFA compliance

8. In order to report on compliance by the police with the provisions of PoFA my predecessors made regular visits to police forces and other law enforcement agencies. The purpose of the visits is not only to find out how forces are applying PoFA in a narrow sense but also to build up a national picture of pertinent, wider issues related to the use of DNA, fingerprints and, increasingly, other biometrics. It is also an opportunity to assist forces by talking through problems, advising where we are able to and sharing knowledge or best practice that we have observed elsewhere. During 2020 my predecessor was only able to visit one body, the National Crime Agency, in the period before the outbreak of the COVID-19 pandemic and the coming into force of the associated government restrictions. As such my office has limited first-hand experience of how the police have used and retained biometrics over this reporting period. My predecessor published an interim report in December 2020 in which he commented upon some basic data that was collected from forces in the autumn of that year.[14]

13 Following an initial retention period allowed for by terrorism legislation – see Appendix C. The period of an NSD was extended to 5 years by the Counter Terrorism and Border Security Act 2019 – see Chapter 2.

14 See Interim Report: https://www.gov.uk/government/publications/biometrics-commissioner-interim-report-december-2020

9. In May 2021, owing to the successful rollout of the COVID-19 vaccine and the corresponding relaxation of government restrictions, I began visiting police forces and intend to visit roughly half of them by the end of the year. This will enable me to report on the level of PoFA compliance across those forces and to observe the impact of COVID-19 on the taking of biometrics. During these visits, we will speak with a range of police staff and officers at all levels including those who work in the force scientific or forensic services department, 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. I will also use this opportunity to discuss their use of surveillance camera systems, their awareness and use of the Surveillance Camera Code and associated issues.

ii. Retention and use of DNA and fingerprints

The governance of national databases

10. The Forensic Information Databases Strategy Board (FIND-SB)[15] monitors the performance of the National DNA Database (NDNAD) and the National Fingerprint Database (IDENT1) 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.[16] FIND-SB brings together DNA, fingerprints and the counter terrorism databases (all subject to regulation by PoFA) within a national governance structure.

11. 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) which is discussed further at paragraph 75.

12. 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 elected local policing bodies[17] who are the voting members. Also in attendance as observers are the Chair of the Biometrics and Forensic Ethics Group,[18] the Forensic Science Regulator, the Biometrics and Surveillance Camera Commissioner, a representative from the Information Commissioner's Office[19] and representatives of the devolved administrations.

13. FIND-SB publishes an annual report which is laid before Parliament[20] 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.

15 Previously named the National DNA Strategy Board until its remit was expanded in March 2016 to include fingerprints. The Board has a statutory basis which is set out in section 63AB of Police and Criminal Evidence Act 1984 (PACE) as inserted by section 24 of POFA.
16 See also Chapter 3, paragraph 186.
17 Police and crime commissioners/police, fire & crime commissioners and others exercising delegated functions on their behalf where there is a mayoral governance model in place as introduced by the Police Reform and Social Responsibility Act 2011.
18 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
19 See http://www.ico.org.uk/
20 See https://www.gov.uk/government/publications/national-dna-database-biennial-report-2018-to-2020

National DNA database

14. The National DNA Database (NDNAD) was established in 1995 and, by the end of the calendar year 2020, held 6,079,575 subject DNA profiles and 631,122 crime scene profiles for England and Wales. This equates to an estimated 5,179,022 individuals. UK holdings total 6,678,369 subject profiles and 660,240 crime scene profiles, or an estimated 5,672,343 individuals.

TABLE 2: Number of DNA profiles held (year ending 31 December 2020)

	Subject Profiles	Crime Scene Profiles	Total
England and Wales[21]	6,079,575	631,122	6,710,697
Rest of UK[22]	598,794	29,118	627,912
Total	**6,678,369**	**660,240**	**7,338,609**

Source: FINDS-DNA

TABLE 3: Total DNA holdings on NDNAD by profile type (year ending 31 December 2020)

	Arrestee	Volunteer[23]	Crime-scene from mixtures[24]	Crime-scene from non-mixtures	Un-matched crime scenes[25]
England and Wales	6,077,518	2,057	135,375	495,747	197,808
Rest of UK	596,508	2,286	2,923	26,195	18,189
Total	**6,674,026**	**4,343**	**138,298**	**521,942**	**215,997**

Source: FINDS-DNA

15. 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, 123,503 in 2019 and 138,298 in 2020) reflects the increasing ability of forensic scientists to analyse such complex stains over recent years.

National Fingerprint Database

16. The National Fingerprint Database became fully operational in 2001 and held all fingerprint sets (tenprints) taken from people 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 which also enabled the storage and search of arrestee palm prints and unidentified palm marks from scenes of crime. In 2007 Scotland began enrolling

21 Includes British Transport Police.
22 Includes Scotland, Northern Ireland, Channel Islands, military police forces and Customs and Excise.
23 '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.
24 Mixed profiles include the DNA information of two or more persons.
25 The number of unmatched crime scenes is included in the crime scene from mixtures and non-mixtures figures.

tenprints obtained for arrests in Scotland to IDENT1 and Northern Ireland began enrolling tenprints in 2013. Currently, fingerprints taken under PACE or its equivalent in the UK are enrolled onto IDENT1 for storage and search.

17. The present Livescan[26] system for the automatic taking and searching of prints came into operation in 2002 and forms part of the Home Office's Biometrics Programme (HOB).

18. The IDENT1 system has been operated by a new supplier since January 2021, bringing IDENT1 and IABS[27] under one service contract. A fingerprint matching platform known as strategic matcher, is due to be rolled out in the next year and will offer a more sophisticated algorithm enabling the identification of matches more quickly and frequently.

19. My predecessor has outlined in previous reports how the statistical information available on the holding and use of fingerprints has never been of the standard and detail as that available for the DNA database. This appears to be because the fingerprint data is collected for contract compliance purposes rather than management information, but it is an unacceptable situation. Work is underway to improve the standard of the available statistical information as part of the transition of the IDENT1 database to a cloud platform and I shall report on progress in my first full annual report next year.

20. IDENT1, as at 31 December 2020, held 26,366,486 sets of tenprints, which relate to 8,452,822 unique arrestee subject tenprint records (i.e. 8.45 million individuals currently have their fingerprints held in the main policing fingerprints collections on IDENT1) and 2,100,736 unmatched crime scene marks relating to 867,876 cases.[28]

TABLE 4: Total holdings on IDENT1 by classification (year ending 31 December 2020)

	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	25,308,233	Data not available	1,798,577	Data not available
Rest of UK	1,158,253	Data not available	302,159	Data not available
Foreign convictions	Data not available	Data not available	Data not available	Data not available
Total	**26,466,486**	**8,452,822**	**2,100,736**	**867,876**

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

26 Livescan is an electronic fingerprint capture system for capturing subject fingerprint and palm print data for enrolment onto the database.
27 The UK National Fingerprint Database for immigration purposes.
28 This data is for the main policing collections on IDENT1.

Additions to NDNAD in 2020

21. The number of DNA subject profiles added to the database has declined over recent years, for example numbers have declined from 540,100 profiles added in 2009/10 to 249,672 profiles added in 2020.[29] There are a number of possible reasons for this, mostly linked to a decline in the number of arrests generally and to the increased use of voluntary attendance for dealing with suspects as an alternative to arrest. This is discussed further at paragraphs 42-43 of this chapter.

TABLE 5: Additions to NDNAD (year ending 31 December 2020)

	Arrestee	Volunteer[30]	Crime-scene from mixtures[31]	Crime-scene from non-mixtures
England and Wales	217,609	No breakdown available	16,905	8,637
Rest of UK	32,063	No breakdown available	713	466
Total	**249,672**	**14**	**17,618**	**9,103**

Source: FINDS-DNA

22. 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[32] and then increased to its present level of 6.67 million. The number of crime scene profiles loaded onto the database has declined from 50,000 in 2008/09 to 26,721 in 2020. My predecessor has previously noted that most forces report having strict procedures in place to ensure that the crime scene investigation resources are focused on serious incidents and those most likely to yield results.

23. In the fiscal year 2019/2, 127,794 subject profile records were deleted from the database[33] and 9,854 crime scene profile records were deleted.[34] I am pleased to hear that a new management information system was rolled out at the end of 2020 and therefore more detailed deletions data will be available from next year.

Additions to IDENT 1 in 2020[35]

24. During 2020, 663,653 unique arrestee records[36] were created on IDENT1 and 257,598 of these were against new individuals. 21,986 crime scene cases were created on IDENT1. A total of 115,320 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.

29 Data supplied by FINDS-DNA. The 2019 figure was similar, with 265,562 subject profiles added to the database during 2019.
30 '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.
31 Mixed profiles include the DNA information of two or more persons.
32 This was in part due to deletions required by the newly enacted PoFA legislation.
33 Including automatic 'PoFA' deletions and deletions under the 'Deletion of Records from National Police Systems' Guidance; see also paragraph 66.
34 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.
35 This data is for the main policing collections on IDENT1.
36 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 2020)

Tenprint sets from arrestees	New Individuals[37]	Unmatched crime scene marks	Cases created with unidentified crime scene marks
663,653	257,598	115,320	21,986[38]

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

25. The global COVID-19 pandemic has had an impact on the volume of tenprints taken from arrestees owing to the logistical challenges of social distancing in custody environments. The Forensics Capability Network released guidance[39] in April 2020 which recommended minimum standards for the taking of biometrics in custody suites during the pandemic which sought to minimise tenprint sampling amongst those whose where there were no questions concerning identity. This has contributed to a reduction in just over 200,000 tenprints sets taken from arrestees compared with 2019 figures.

Deletions from IDENT1 in 2020

TABLE 7: Deletions from IDENT1 (year ending 31 December 2020)

Tenprint sets from arrestees	Individual subjects	Unmatched crime scene marks	Cases with unidentified crime scene marks
140,384	38,731	166,344	Data not available

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

26. During 2020, 38,731 individual PACE subject records and 166,344 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 Police National Computer (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.[40]

Police National Computer (PNC) deletion error

27. In January 2021, an error with the PNC caused the system incorrectly to highlight a large number of fingerprint records for deletion, approximately 30,000 of which were deleted before the error was detected and deletions paused. This, in turn, caused DNA records to be deleted from the NDNAD owing to erroneous messaging from the PNC. The Forensic Information Databases Service (FINDS) has confirmed that it will be possible to recover all of the lost records, however this work is still ongoing. Whilst it is helpful that these biometric records can be recovered from back-up data, their recoverability calls into question how effective the 'deletion' processes really are and whether biometric data is

37 Number of new individuals rather the number of individuals against print numbers – different to previous years.
38 Cases created may not be filed to the database.
39 See https://www.fcn.police.uk/latest/coronavirus
40 Or the case is required to be deleted according to the Management Of Police Information (MOPI) rules.

being either properly deleted or unnecessarily duplicated in line with the relevant legislation which is principally a matter of public confidence. I have raised this with the Information Commissioner's office. Whilst there may be very good reasons for retaining back-up data systems, this needs to be clearly explained and communicated to the public whose legitimate expectation will be that their biometrics are permanently deleted in accordance with statutory retention periods.

Speculative searches

28. The police have a power 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*.[41] 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, allowing tenprint sets to be searched against one or more collections of fingerprints on that database immediately, 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.

29. 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. The Metropolitan Police Service is however exploring the use of a new DNA profiling capability in custody suites which could significantly reduce the turnaround time for DNA profile match reports.

Match rates – DNA

30. The extent to which crime scenes are examined for DNA stains varies significantly between offence types. This is because the likelihood of DNA being found at a crime scene varies by offence and, in addition, more serious incidents are likely to be prioritised.

31. Given that most of those convicted of a recordable offence will have their DNA and fingerprints retained,[42] biometrics will be available to police investigators for most individuals who reoffend. Repeat offenders make up a significant proportion of overall offending. As a result, the rate at which crime scene profiles produce a match to subject profiles held on the database is high (presently 66.13% for England and Wales in 2020 which is fractionally lower than last year).

41 PACE 1984 section 63D(5).
42 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 8: Match rate for matches obtained immediately on loading for England and Wales forces (year ending 31 December 2020)

	Crime Scene to Subject Profile	Subject Profile to Crime Scene
Total Loaded	26,721	249,672
No. of Matches	17,646	5,263
Match Rate	66.13%	2.13%

Source: FINDS-DNA

Match rates – fingerprints

32. 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 data availability issues. 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.

TABLE 9: Fingerprint matches during 2020

	Scene of crime palm mark to palm print	Scene of crime fingermark to tenprint	Tenprint to scene of crime mark
Total searches	70,109	401,957	Data not available
Number of matches	3,876	17,281	Data not available
Match rate	01:18.1	01:24.3	02:53.9

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

iii. Footwear impressions

33. There is much discussion, professionally and publicly, as to what qualifies as 'biometrics'. A useful working definition can be found in the four broad features that some researchers see as being essential for any reliable biometric personal identifier:[43]

1. Collectability (the element can be measured);
2. Universality (the element exists in all people)
3. Unicity (the element must be distinctive to each person);
4. Permanence (the property of the element is permanent over time)

43 See Mordini, Emilio and Sonia Massari (2008) Body, biometrics and identity, Bioethics 22(9): 489 in Boy, Jacobsen & Lidén, Societal Ethics of Biometric Technologies, Societal Ethics of Biometric Technologies (2nd edition), 2018.

34. In light of the widespread attention that has been attracted by the lack of statutory regulation of 'new biometrics' and databases of facial images some may find it surprising that, despite their being clothing and lacking three of the four biometric elements above, footwear impressions are included in the PoFA regime and are regulated by the Police and Criminal Evidence Act 1984 (PACE).

35. Section 63S(3) of PACE[44] states:

> *"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."*[45]

36. 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).

37. 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.

38. 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.

39. There is currently no agreed national policy or approach to the retention of footwear impressions by all police forces in England and Wales.[46] Some forces have reported regular use of footwear impressions, whereas others do not routinely collect them as other investigative tools are considered more cost-effective. The processing can also greatly vary been forces i.e. some forces upload the images of marks from scenes to the NFD, others upload images of the prints taken from footwear and others simply do not upload their footwear impressions to NFD. I have raised the area of footwear impressions with the new Forensic Science Regulator.

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

40. The Protection of Freedoms Act 2012 provides a specific legal framework for the police retention and use of biometrics (DNA and fingerprints) largely by amending the Police and Criminal Evidence Act 1984 (PACE) which is the principal statutory source of police powers and procedures in this area. However other legislative changes to PACE and associated statutory codes have had significant consequences for both the taking and retention of biometrics which my predecessors have outlined in detail in previous annual reports. There are two key statutory changes which are continuing to have an impact on the biometric regime under PoFA:

---

44 Inserted by s.15 PoFA.
45 See: http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/1/enacted
46 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.

A. The Police and Criminal Evidence Act 1984 was amended in 2005[47] to introduce criteria which a police officer must believe make the arrest of a person *necessary* before the officer can use the general power of arrest under s.24. In November 2012, Code G of the PACE Code of Practice changed in response to a number of decisions in which the courts clarified the law on the *necessity* of arrest.[48] In particular:

   i Where a police officer needs to interview a suspect, they must 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 Police and Criminal Evidence Act 1984 was further amended in 2017[49] to introduce 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.[50]

41. Both of the above statutory amendments to PACE were made partly in response to reducing the level of intrusion into the individual rights of those suspected of involvement in criminal offences. However, they have had a – probably unintended – effect on the efficacy of the PoFA provisions as set out below.

A. Voluntary attendance

42. Since the 2012 changes to Code G, the use of arrest has gradually declined (in line do doubt with the policy intent behind it) and police forces are now routinely using alternatives to arrest in around one third of cases where suspects are questioned. Suspects who are not arrested are asked to attend voluntarily, usually outside a custody suite environment, to answer questions and are commonly known as 'voluntary attendees' (VAs).

43. NPCC national guidance 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). However, there remains the practical problem that the opportunity lawfully to take biometrics frequently occurs long after the suspect has left the police interview. My predecessor observed that some forces have made considerable improvements to their processes to ensure that biometrics are captured appropriately from VAs. However, others have not implemented robust monitoring[51] and many were not able to provide relevant data in autumn 2020. It seems from this reporting that the COVID-19 pandemic exacerbated this issue.[52] This is significant as the value of national databases of both convicted offenders and unsolved crime scene stains against

47 By the Serious Organised Crime and Police Act 2005, s. 110.
48 *Richardson v The Chief Constable of West Midlands Police:* QBD 29 Mar 2011.
49 By the Policing and Crime Act 2017.
50 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.
51 Forces have commonly reported that their IT systems do not allow them capture VA data.
52 See guidance published by the Forensic Capability Network in April 2020 outlining that the procedures for taking biometrics from detainees.

which a suspect's biometrics may be speculatively searched inherently reduces when there is a reduction in taking of biometrics. I intend to engage with forces on their use of VA during my visits this year and will comment further on these issues in my next report.

B: Bail and 'released under investigation'

44. The introduction of the overriding presumption of release without pre-charge bail (unless strict necessity and proportionality criteria are met) changed the way in which suspects are released from police custody. When the changes first came into effect in April 2017 the number of suspects being released on bail reduced to almost zero. Since then, the use of pre-charge bail has increased, although the majority of suspects whose investigations are ongoing continue to be 'released under investigation' (RUI).[53]

45. My predecessor outlined the impact of this legislative change on the retention of biometrics by the police. He observed that RUI cases were often not monitored rigorously and that some remained open for lengthy periods, in contrast with those where the suspect is released on pre-charge bail because there are strict oversight and reporting requirements on bail cases which are not applicable to RUIs. He also reported that many forces faced IT challenges and had been unable to update their systems resulting in PNC records not being automatically updated when an investigation ended. This is significant as specific updates to PNC records cause biometrics to be deleted from the databases, creating a risk that biometrics would be held unlawfully.

46. Data collected from police forces in autumn 2020 indicates that some forces have now managed to implement the IT and process changes required to enable the effective monitoring of RUI cases, although for others this continues to be an issue. In February 2020 the Home Office launched a consultation on pre-charge bail which included the proposal to end the presumption against it. The Government's response to the consultation's findings, issued in May 2021, confirms the intention to legislate to remove the presumption and to make it easier to use bail in cases where it is necessary and proportionate.[54] This will create a neutral position within the legislation so that there is neither a presumption for nor against pre-charge bail. I intend to discuss the use of bail and RUI with police forces during my visits over the coming year, as well as any potential operational implications of further legislative change.

Implementation of legislative change affecting biometric retention based on convictions outside England and Wales

47. If a person is arrested in England and Wales (E&W) and, subsequently, no further action is taken in relation to the arrest offence, their DNA and fingerprints may be retained if they have a previous conviction for a recordable offence (see paras 6-7 for full biometric retention rules). When PoFA was originally passed, it laid down certain conditions for retention where a conviction had occurred outside E&W. First, the conviction must be equivalent to a qualifying offence in E&W. Secondly, the biometrics must have been taken in relation to that conviction. These conditions made the power difficult to use, so the Policing and Crime

53 In the 2019 Annual Report my predecessor noted that those forces which were able to provide the relevant data reported using bail in roughly 10% of investigations.

54 See p.10: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/953715/2021-01-14_Response_to_PCB_consultation__003_.pdf

Act 2017 replaced them with a provision allowing retention on the basis of any conviction in another jurisdiction, where 'the act constituting the offence would constitute a recordable offence if done in E&W'.[55]

48. I was surprised to learn at the FIND-SB meeting in April 2021 that, four years on, this legislative change has yet to be implemented on the PNC. It is almost invariably the case in the area of biometrics that the plea is for the law to keep pace with the technology but in this instance the legislative changes sought at the time have waited for several years for the technological solution to catch up. This considerable delay clearly creates a risk that the police lose biometrics that may have proven critical to a criminal investigation; it also has the wider potential to undermine the case for future legislative change.

v. Processing and storage of DNA samples

Sampling errors

49. 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 correctly applied or the swab correctly placed in the tube. The sample is then submitted to a Forensic Service Provider (FSP) for profiling. Forensic Service Providers 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.

50. Since April 2016, data has been collected for the FIND-SB on errors in DNA sample handling by police forces of people in police detention; the collection of crime scene sampling error data is intended to commence later this year. Since 2019, all forces have provided data on errors identified in force and those errors are categorised in a uniform way. Similar to 2019, by far the most common error during 2020 was simply failure to seal the bag containing the DNA sample, accounting for nearly 30% of all reported errors. Administrative errors may also occur which mean that profiles cannot be loaded to the database. In England and Wales around 1% of profiles could not be loaded for this reason in 2020. Samples may also be lost by forces, although this happens very rarely (c. 0.6% of samples). It is however concerning that there are still a handful of forces that have not been able to report to FINDS the number of 'lost samples' this year.[56] More positively, 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.[57] These errors occur in around 0.05% of all subject profiles loaded to the NDNAD.

51. Sample or record handling errors made by police forces when taking subjects' DNA samples can have 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

55 See: https://www.legislation.gov.uk/ukpga/2017/3/section/70/enacted
The 2017 Act only made this change for biometrics taken under PACE in E&W, not for those taken in the devolved administrations or the islands.

56 Bedfordshire, Cambridgeshire, Hertfordshire, Greater Manchester, Surrey, Sussex and Thames Valley Police have not been able to provide this data to FINDS.

57 These occur when the DNA profile is associated with the wrong information.

subject, the potentially important DNA data is lost.[58] The forces I have visited have formal processes and policies in place relating to DNA sampling failures. I shall continue to review this with the other forces I am due to visit this year.

52. 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. If these errors were not to be identified, there is a small chance of a miscarriage of justice however 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

53. 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 (FSPs): Key Forensic Services, Eurofins Forensic Services and Cellmark Forensic Services. There have been some serious concerns, particularly over the past four years, about the stability of the forensic marketplace in England and Wales which have been discussed in the annual reports published by the former Forensic Science Regulator.[59] During my visits forces have explained that caps on the number of samples that can be sent to an FSP at any one time can create significant backlogs. In Scotland and Northern Ireland similar forensic services are provided by the Scottish Police Authority Forensic Service and Forensic Science Northern Ireland.

Destruction of DNA samples

54. There are clear rules in PoFA as to when biometric samples should be destroyed.[60] Whilst PoFA allows the police to take DNA samples from all people 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 reflect Parliament's decision that the information contained in a person's DNA sample was so sensitive that once the police had derived a DNA profile for criminal justice purposes the sample should be destroyed. However, other legislation allows the police to keep DNA samples until a criminal investigation and allied disclosure arrangements are concluded. This is an exception under the Criminal Procedure and Investigations Act 1996 (known as the CPIA exception).[61]

55. 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. I have yet to visit the FSPs, however all the evidence seen by my predecessor confirmed that they 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

58 At the very least additional police resources are needed to re-take the sample from the subject (who may well have left police custody).
59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868052/20200225_FSR_Annual_Report_2019_Final.pdf page 11.
60 For details and discussion, see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015*, at Section 4.1.
61 Section 63U(5)of PACE 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 and 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.

stores. Individual forces have responsibility for monitoring these samples and ensuring that they are destroyed in a timely manner. This is an area I will cover in each of the police force visits I undertake.

CPIA exception

56. As outlined above, the general rule introduced by PoFA is that DNA samples should be deleted as soon as a DNA profile has been derived and 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"*.[62] 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.[63]

57. 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 provide quarterly data returns to FINDS which include the number of both PACE and elimination samples they are retaining 'in force' under the CPIA exception. The FSPs provide this information to FINDS for samples that they have been asked to retain, on a monthly basis.

58. 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).

59. Since January 2016, all elimination samples have been subject to the same retention rules as those taken from individuals arrested for recordable offences.[64]

60. In May 2021, I wrote to all chief officers and their elected local policing body following a meeting of the Forensic Information Databases Strategy Board (FINDS-SB) where it was noted that there have been significant difficulties in obtaining quarterly data returns from some forces on their CPIA holdings. These returns allow me to have oversight of the use of this exceptional retention power and ensure DNA samples are only retained if the necessary criteria are met in accordance with PoFA. As well as reminding forces of the importance of these returns, I underlined that the CPIA provision is a provision of exception and should not be used as a general retention for certain types of offences. My office has observed, through data requested at the end of 2020, that there remains significant variation in the extent to which forces are using the CPIA exception to retain DNA samples with some continuing to retain high numbers of samples under the authority of the CPIA. While no official guidance

62 *Loc cit.*
63 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.
64 For further discussion of volunteer samples see: *Commissioner for the Retention and Use of Biometric Material, Annual Report 2016, 226-231.*

has been issued on the use of the CPIA exception, my predecessor wrote to forces in 2017 and usefully set out suggested principles for its use[65] which I have again brought to the attention of police forces.

61. The last quarterly report received by my office in 2020 provides the retention figures for DNA samples held under CPIA 'in force' and with FSPs as at 31 December 2020. These are set out below (Table 10).

62. My predecessor has previously noted that several forces have applied a blanket retention policy for DNA samples taken following certain types of offence, most commonly sexual offences, in case further analysis of the sample is required. In some cases involving an allegation of a sexual offence further analysis of the DNA sample (most commonly Y-STR Analysis[66]) will be necessary, however this is not generally applicable to all samples taken in relation to all sexual offence allegations. This is because DNA analysis is not usually relevant to the issue of consent, for example, which is often the key issue in the majority of sexual offence allegations. I will continue to discuss with forces their use of the CPIA exception in the course of my visits this year and monitor the numbers of DNA samples they are retaining via their returns to FINDS.

TABLE 10: DNA samples held under CPIA by England and Wales forces (year ending 31 December 2020)

	Total		Held in Force		Held by FSPs	
	2019	2020	2019	2020	2019	2020
Arrestee/ PACE samples	7,070	6,424	899	654	5,880	5,770
Elimination samples	3,796	2,970	2,526	3,063	1,270	1,091

Source: FINDS-DNA

Copies of DNA profiles and fingerprints

63. The provisions governing the retention and use of copies of fingerprints and DNA profiles are contained in section 63Q of PACE (as amended by PoFA). Copy fingerprints are retained in the National Fingerprint Archive and by some police forces in their archives. I am not aware of any reason to suspect significant non-compliance with section 63Q of PACE.

65 A copy of this letter can be found in an Appendix D to the 2018 Annual Report: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2018

66 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

vi. Deletion of Police Records

Applications for PNC record deletion

64. Individuals 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).[67] This is referred to as the 'Record Deletion Process' (RDP). 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. The RDP allows individuals to make an application for deletion of their PNC record and associated biometrics in respect of out of court disposals, NFA disposals[68] and non-conviction disposals issued in court. Individuals who have been issued a Court Conviction, either as an adult or juvenile, are not eligible to apply under this 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 decides whether the information should be retained or deleted.

65. Although not a mandatory requirement for application, individuals are encouraged to provide reasons why their record(s) should be deleted under the ground(s) stated in their application. This will support their request for deletion and enable the force to conduct a thorough review. The ACRO Information Management Unit is responsible for coordinating requests for record deletion and will contact applicants where the grounds for record deletion have not been fully evidenced to give the applicant the opportunity to provide additional information to support their request.

66. The decision whether a record is retained or deleted from national police systems is at the discretion of the chief officer of the relevant police force (taking into account the national guidance[69] issued in respect of this process). My predecessor observed from visits to police forces and the data supplied on the number of deletions approved by chief officers that there was significant variation in the application of this guidance from force to force.

67. During the year ending 31 December 2020, 671 deletions were approved by chief officers (see Table 11 below). This is compared to 923 such deletions approved by chief officers in 2019 and 658 in 2018. It is noteworthy that these deletions represent a very small proportion of those records that are potentially eligible for deletion. I also note that there continues to be a larger number of decisions pending with forces, which may reflect the availability of police resources, particularly during the COVID-19 pandemic.

67 Public guidance on submitting an application for the early deletion of these records is published on the ACRO website: https://www.acro.police.uk/Record-deletion

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

69 An updated version of the guidance 'Deletion of Records from National Police Systems (PNC/NDNAD/IDENT1) was published in April 2020: https://www.acro.police.uk/ACRO/media/ACRO-Library/Deletion-of-Records-from-National-Police-Systems-(Guidance)-v2-1-April-2020.pdf

TABLE 11: Records deletion process (year ending 31 December 2020)

	Total Applications received by ACRO Records Deletion Unit	Approved by Force	Partially approved by force	Rejected by Force	Rejected as ineligible by ACRO Records Deletion Unit	Pending with Force	Pending with Applicant
2019	2,230	923	41	803	436	27	0
2020	2233	671[70]	25	566	454	497	20

Source: ACRO Criminal Records Office – Records Deletion Unit

Review of criminal record retention rules

68. In March 2021 the National Police Chiefs' Council launched a consultation as part of the PNC Retention and Disposal Review with a view to ensuring that the criminal record retention rules on the PNC (and the system that will replace it) protect the rights and freedoms of the citizens of England and Wales, while preserving policing and law enforcement's ability to discharge their duties in managing threat, harm and risk in order to protect and safeguard the public. The consultation proposes a set of rules which move away from the blanket retention of criminal records until the relevant individuals reach 100 years of age, replacing this with a policy which takes into consideration the age of individuals at the time of an offence (or alleged offence), the seriousness of the offence and the outcome recorded for the investigation.

69. These proposed changes impact on biometric retention as the relevant police systems are linked; the disposal of a PNC record triggers the deletion of any associated biometric data. Once implemented, these changes should bring PNC retention policies into line with the legal framework protecting human rights and data protection. As part of my response to the consultation I have queried how historical records will be dealt with under this new policy. To avoid undermining its integrity, the deletion of historical records should be factored in as opposed to offering people the right to request deletion as is currently the case with custody images.

Custody images

70. 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.[71]

70 Figures only accurate as of the date they were provided (22.02.2021).
71 *R(RMC and F) v Commissioner of Police of the Metropolis* [2012] EWHC 1681 (Admin).

71. The Home Office responded to this judgment by publishing, in 2017, a Review of the Use and Retention of Custody Images.[72] The Review reiterated that the time periods for reviewing information about an arrestee as set out in MoPI, depending on the offence, should be applied specifically to custody images. It also introduced a right for an arrestee to make a request to a chief officer for their facial image to be deleted, with a presumption in favour of deletion in certain, limited circumstances.

72. The College of Policing has since issued a recommended process for responding to requests to chief officers for the deletion of facial images which is published on their website.[73] My predecessor observed from his visits to police forces across England and Wales 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 (discussed above at paras 64-67) as the application form for that process includes a 'tick box' for custody image deletion. I have recommended to the police forces I have visited that they put in place measures to inform individuals upon leaving custody of their rights in relation to requesting deletion of their custody image.

73. My predecessor also commented that police forces throughout England and Wales had found 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 existing IT systems. As a result, few were carrying out the active reviews required by MOPI and most were continuing to retain the vast majority of their custody images indefinitely, regardless of whether the individual has been convicted of an offence.

74. I am aware that the Home Office is exploring policy and technical options to enable the automated deletion of custody images and is engaged with the recently established NPCC Custody Image Compliance group as part of this work.[74] In advance of the implementation of automatic deletion, guidance has been developed to help individuals understand their rights when it comes to requesting deletion of their custody image which will soon be made publicly available. These efforts to improve transparency and public access to information are welcome, however it is concerning that a viable technical solution will not be implemented in the near term meaning that the onus remains on individuals to 'opt in' for their image to be considered for deletion by the police. It is clear that the rectification of this situation represents both a technical and a legal problem for police forces. Notwithstanding the practical challenges of deletion, it is important that police forces are able to provide assurance that the retained images are not used inappropriately.[75] It is also interesting to note that there are people who want changes in the law to prevent the police using automated decision-making in facial databases. As the effective deletion of the custody images cannot be achieved *without* automated decision-making this provides a small example of how technical complexity and public trust may pull in different directions simultaneously (and how outright bans can produce unintended consequences). More broadly, this is just one part of the complex police database picture and it is important that the public are able to have trust and confidence in the whole 'ecosystem' rather

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

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

74 Home Office Ministers are due to provide evidence on these matters to the House of Commons Science and Technology Committee in June 2021.

75 For example, the custody image database may be the source of images for watchlists used to conduct live facial recognition (LFR) or used to compile images used in video identification parades. See the ICO report on how the police use facial recognition technology in public places, p.18-20: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

than discrete offshoots. Increasing the public's confidence in the way their information is managed generally is a stated purpose of the Police Information and Records Management Code of Practice which is intended to replace MOPI and on which a consultation was launched in early 2021.[76] I welcome this clear expression of strategic purpose and look forward to seeing the revised statutory Code.

vii. HOB databases and LEDS

75. Following the Bichard Inquiry Report[77] into the Soham murders, a new database – the Police National Database (PND) – was created 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 the inquiry. 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 18.5 million facial images[78] of which around 14.5 million are technically suitable and of sufficient quality to be searchable.[79]

76. The Home Office is in the process of replacing legacy databases via the Home Office Biometrics Programme (HOB). HOB will replace existing Home Office biometric databases such as the national fingerprint database, IDENT1, and its sister programme, the National Law Enforcement Data Programme (NLEDP), will replace the Police National Computer (PNC) with the single Law Enforcement Data Service (LEDS). I understand that there have been significant problems with NLEDP which has recently undergone a full review of its scope, architecture and delivery approach. As a result, it will now deliver new capability incrementally and the replacement of PND has been removed from its scope, with a separate project in place to keep this database operational over the next 5 years. Starting with the first capability this year, the delivery of full LEDS functionality is not expected until 2025.

77. 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 enabling different governance rules to be applied for the use of, and access to each collection.

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

78. In response to investigations of certain serious offences the relevant chief officer of police may apply to retain biometric material lawfully taken in the course of the investigation. The application may be made under the Police and Criminal Evidence Act 1984, either in respect of the special characteristics of the victim/complainant or their relationship to the suspected offender (section 63G(2)) or the general prevention and detection of crime (section 63G(3)).

76 https://www.college.police.uk/article/information-records-management-consultation
77 https://Dera.ioe.ac.uk/6394/1/report.pdf
78 This figure does not include images of marks, scars, tattoos which are also held on PND.
79 Figures provided by PND Service Desk.

79. The legislation states that an application may be made under section 63G(2) if the material was taken in connection with the investigation of an offence where the alleged victim was under the age of 18, vulnerable or associated with the person to whom the material relates. Alternatively, an application can be made under section 63G(3) if the material does not fall under subsection 2, but the responsible chief officer of police considers that the retention of the material is *necessary* to assist in the prevention or detection of crime.

80. In reviewing my first batch of cases as Commissioner, a common theme that emerged was that police applications made under 63G(3) did not always appropriately set out the reasons why the retention of the subject's biometrics is *necessary*. I have accordingly challenged police forces to provide further justification before taking a decision on these applications. My office has also issued communications to police forces highlighting the need to pay particular attention to the necessity test to avoid delays.

81. Between 31 October 2013 and 31 December 2020, 459 applications were made in relation to victim characteristics and 314 were made for the more general purpose of the prevention or detection of crime.[80] In some cases more than one of the 'victim criteria' were satisfied.

TABLE 12: Statutory basis for applications to the Commissioner (31 October 2013 – 31 December 2020)

	Applications received[81]	Approved	Refused
Victim criteria[82]			
– under 18	334	204	128
– 'vulnerable'	34	22	11
– associated with subject of application	91	33	57
Prevention/detection of crime	**314**	**228**	**86**

80 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 clearly set out and satisfied, my office has treated the application as if it were being made under that provision.

81 Including cases invalid or withdrawn.

82 In some cases more than one of the victim criteria are satisfied.

TABLE 13: Number of applications to the Commissioner by force (Year ending 31 December 2020)

Force	2020	Total Applications since 31 Oct 2013
Metropolitan Police	53	418
Yorkshire and Humberside[83]	17	86
Thames Valley	8	29
South Wales	7	24
Essex	6	22
Devon and Cornwall	5	21
Hampshire	3	8
Kent	3	29
Avon and Somerset	2	7
Cleveland	2	6
Hertfordshire	2	10
Cambridgeshire	2	16
Northumbria	1	22
Bedfordshire	1	7
Durham	0	4
Gwent	0	3
Northamptonshire	0	2
Cumbria	0	2
Dorset	0	9
Derbyshire	0	1
Gloucestershire	0	1
Greater Manchester	0	3
Lincolnshire	0	1
Norfolk	0	1
North Wales	0	4
Warwickshire	0	4
West Mercia	0	6
Wiltshire	0	1
TOTAL	**112**	**747**

83 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 2019	1 January 2020 to 31 December 2020
Total Applications	**635**	**112**
– Representations from subjects	73 (11%)	9 (8%)
Outcomes		
Approved	422 (66%)	77 (69%)
Rejected	146 (23%)	29 (26%)
Withdrawn	64 (10%)	5 (4%)

Preliminary applications

82. 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 submitting a formal application or notifying the subject of the application.

83. In fact, matters of disclosure have arisen only relatively rarely and up to 31 December 2020 only 17 such applications have been made. All bar one of these preliminary applications have gone on to become full applications.

Applications to a District Judge

84. Whilst I can consent to the retention of biometrics for those arrested for, but not charged with, a qualifying offence, the applicable 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.[84]

85. In the last Annual Report, it was 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.[85]

The applications process

86. Applications are made electronically by the police who must provide details of the case and 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. The police must notify the subject by letter detailing the application and the reasons for it being made. Where the subject is under 18 years of age, an appropriate adult is also

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

85 It is interesting to note that under the Scottish system, all such applications must be made to a sheriff and there is no record of any such application ever having been made since the establishment of Police Scotland in 2013. See Section 18A Criminal Procedure (Scotland) Act 1995 as inserted by the Police, Public Order and Criminal Justice (Scotland) Act 2006.

identified and notified of the application so that the young person,[86] in particular children, will be able to understand the process and make well-reasoned representations if they wish to do so. Some police forces were not always fulfilling this requirement and my office redistributed guidance in the autumn of 2020 as a reminder. Since then, the vast majority of applications have followed the correct process.

87. In every instance, the subject (and appropriate adult if applicable) of an application is told whether 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 my office.[87] The submission of representations is taken as both confirmation of the subject's contact details 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 (and appropriate adult if applicable) 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 within 28 days of the decision date.

88. 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 sent but is instead 'served to file'.

On what grounds does the Commissioner decide applications?

89. The police have to demonstrate that, whilst the person who is the subject of the application was not charged with the offence, there is evidence supporting the likelihood that they were involved in the offending, 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 with the subject's right to respect for a private and home life is proportionate given the public benefit that is likely to result. I must weigh the evidence presented against each of these factors, in each case, before reaching a decision. The core principles and approach to assessing are set out in a guidance document issued by FIND-SB called *Applications to the Biometrics Commissioner under PACE*.[88]

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

- the available evidence is unlikely to support a successful prosecution[89] or
- charging the subject would not be in the public interest.[90]

91. 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 'charging threshold' used by the CPS to decide whether to charge requires the available evidence to be such that there is a realistic prospect of conviction. This turns on how far the evidence is likely to meet the requirements

86 Following NPCC guidance issued at the end of 2019.
87 Since the conclusion of the 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.
88 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).
89 See http://www.cps.gov.uk/victims_witnesses/reporting_a_crime/decision_to_charge.html
90 See http://www.cps.gov.uk/victims_witnesses/reporting_a_crime/decision_to_charge.html. 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.

of the criminal trial process. In many cases a principal reason for the decision not to charge is the withdrawal of a complainant's statement or reluctance for an independent witness to provide a formal statement, often as a result of fear of reprisals. As I am not bound to consider the evidence against the subject to the higher criminal standard of proof, I require that the criteria as set out in the guidance document are satisfied and that retention of the subject's biometrics is 'appropriate' in that light.

92. I also have to be satisfied that retaining the biometrics will reduce the risk of, or deter further offending, or will help in the detection of crime. For example, in relation to some crimes, biometrics are *often* of importance in identifying the offender and associating them with the crime scene (e.g. burglary), for others they *may* be (e.g. sexual offences where identity is in issue) and others *rarely* (e.g. domestic violence where the suspect and complainant still live together).[91] It is for the police to provide sufficient information demonstrating that, in the particular circumstances, retaining the subject's biometrics is appropriate.

93. Even if both 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 with individual freedom that it will involve. Where the subject is under the age of 18 I must consider that *'particular attention should be paid to the protection of juveniles from any detriment that may result from the retention … of their private data'.*[92] Failure to meet any of these conditions will lead me to refuse an application.

What type of offences lead to applications?

94. The police may only make applications in relation to 'qualifying offences'. As can be seen in Table 15, the majority (60%) of applications have been made for sexual offences.

TABLE 15: Outcome of applications to the Commissioner to retain biometrics for qualifying offences under section 63G PACE (31 October 2013 – 31 December 2020)

Offence Group	Total applications	Approved[93]	Refused[93]	Withdrawn[93]
Murder, Attempts and Threats to Kill	15	7 (46%)	7 (46%)	1 (7%)
Sexual Crimes	429	259 (60%)	131 (31%)	39 (9%)
Assaults	121	90 (74%)	15 (12%)	16 (13%)
Robbery	105	84 (80%)	11 (10%)	10 (9%)
Burglary	58	46 (79%)	11 (19%)	1 (2%)
Other	19	14 (74%)	1 (5%)	4 (21%)
Total	**747**	**500**	**176**	**71**

91 The Domestic Abuse Act 2021 received Royal Assent on 29 April 2021 to strengthen measures to prosecute perpetrators of domestic abuse and improve criminal justice outcomes for victims. See: https://www.legislation.gov.uk/ukpga/2021/17/contents/enacted. The potential impact of these wide statutory provisions on s.63G applications is difficult to predict.

92 Per *S and Marper v United Kingdom* (2008) 48 EHRR 1169 at paragraph 124.

93 Figures may differ from previous annual reports to better reflect updated accurate data.

95. The high percentage of sexual offences is indicative of the evidential and procedural challenges involved in these types of case. Often there are no independent witnesses and many cases involve uncorroborated allegations made by one party against another. My predecessor commented on the peculiar complexities of applications for alleged sexual offences which take place in the family context where the identity of the alleged offender is not in doubt and the utility of retaining biometrics is thereby diminished.[94]

96. Over the past year my office has processed a number of applications where sexual contact is confirmed to have taken place, but the key fact in issue is whether it was consensual. This reflects the evidential requirements of these types of case, however all applications depend on the individual circumstances of the case and the level of detail provided by the chief officer.

97. My office has previously examined recidivism rates amongst individuals who have been the subject of a section 63 application. That analysis was published as Appendix E of my predecessor's 2018 Annual Report.[95] I hope to continue this analysis in building a knowledge base to assist the police in deciding which cases are most worth pursuing and to assist in understanding the effect of the legislation.

Why do so few subjects of applications challenge the police case to the Commissioner?

98. Parliament was careful in legislating to allow the subject of an application to challenge that application by making representations but to date only a small minority of the subjects have done so – see Table 16

TABLE 16: Representations by subjects and outcomes (year ending 31 December 2020)

Applications	Totals	Representations made by the Subject of the Application[96]
Approved Applications	500	46 (9%)
Refused Applications	176	33 (19%)

99. It is conceivable that subjects may not, as a representative group, be highly literate, informed, well-resourced and/or may find the task of challenging the case advanced by the police daunting and bureaucratic.[97] Subjects may also believe that they will not be listened to or that they simply wish, following an NFA decision for an alleged offence, to bring to an end what has probably been a lengthy and stressful experience. Whatever the causes, the low rate for the submission of representations suggests that this particular provision for protecting subjects of an application is not working as expected.

94 See Annual Report 2019 (paragraph 203-208): https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019
95 See Annual Report 2018 Appendix E: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2018
96 Figures may differ from previous annual reports to better reflect updated accurate data
97 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.: https://discovery.ucl.ac.uk/id/eprint/1531971/1/Creese_10.18546_LRE.14.3.02.pdf

100. Subjects are told how to make representations when the police notify them about the application. They (or their appropriate adult/legal representative) can do this by writing to my office which continues to be the most common way to make representations, but they may also make representations by telephone.[98] Instructions on making representations and the notification letter have previously been revised to simplify the process and encourage subjects to make representations. Unfortunately, there been no increase in representations, with only 9 subjects doing so in 2020 in written format. Since introducing the telephone option my office has received only 2 representations in this way. I will continue to monitor the arrangements and how we might make the representation process easier.

Section 63G – a process-model?

101. Reflecting on my first six months as Commissioner, I have been particularly impressed by the operation of the regime established under PoFA for processing and determining applications made under S63G. Notwithstanding the issues around take up for the making of representations discussed above, the 63G process offers a model by which the police and other agencies might apply to retain and use other biometric material in a way that involves clear legal limitations and criteria, transparency, independent oversight and the opportunity for challenge falling short of a formal application to a court.

Biometrics Commissioner 'UZ' markers

102. If a chief officer is minded to make an application under section 63G of PACE they have until 14 days after the 'NFA date' to put an appropriate 'marker' on the PNC (a 'UZ' marker) which will stop the automatic deletion of the relevant biometric records. This marker remains in place 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 with a monthly report by ACRO Criminal Records Office (ACRO) 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.

98 The ability to make telephone representations was impacted upon by the COVID-19 global pandemic owing to staffing and we have encouraged subjects to contact us electronically if they wish to make telephone representations.

103. As of December 2020, a total of 207 UZ markers were in use by forces in England and Wales. That figure breaks down as follows:

TABLE 17: Biometrics Commissioner 'UZ' markers by Force (January 2021)

Metropolitan Police Service	68
South Wales Police	18
Cambridgeshire Constabulary	16
Thames Valley Police	11
Devon & Cornwall Police	11
West Yorkshire Police	10
Humberside Police	10
Northumbria Police	8
Bedfordshire Police	7
Hampshire Constabulary	7
Essex Police	6
Gwent Police	6
South Yorkshire Police	5
Cleveland Police	5
West Mercia Police	3
Hertfordshire Constabulary	3
Avon and Somerset Constabulary	3
Dorset Police	3
Kent Police	2
Durham Constabulary	2
North Yorkshire Police	1
City Of London Police	1
North Wales Police	1
Total	**207**

104. 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 without any application for retention having been made to my office. Both present a risk of the biometrics being retained unlawfully and a further, wider risk to public confidence in the retention and use of biometric material by the police. My office reviews the markers on a bi-monthly basis and will continue to keep this under close review to ensure UZ markers are correctly applied.

2. Biometrics and National Security

105. 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 (CT) Command and in Northern Ireland by the Police Service of Northern Ireland (PSNI). The majority of CT 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

106. 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:[99]

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)[100] 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 same way as they would for any other arrestee.[101]

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.[102]

iii Schedule 7 to 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.[103] 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 to the same Act[104] (see also paragraph 108 below).

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

107. A significant proportion of the biometrics of which I have oversight are taken when someone is stopped and detained under Schedule 7 powers. It is clear to me from the cases I have overseen during my short time in post that these powers are an invaluable CT tool without which the National Security Determination (NSD) regime described below would not be effective. 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

99 See also Appendix C.
100 PACE section 24.
101 See also Chapter 1, paragraph 5.
102 http://www.legislation.gov.uk/ukpga/2000/11/schedule/8
103 As defined in TACT section 40.
104 http://www.legislation.gov.uk/ukpga/2000/11/schedule/8

person. As my role does not include oversight of the Security Service, I am restricted in the information that is made available to me about what is known about these individuals (see also paragraphs 109-115 below).

108. Biometrics are not taken in every case of an individual being detained under Schedule 7 powers and there is guidance for officers to assist officers in deciding whether to take biometrics. 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. 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[105] for designated specific reasons.[106]

Biometrics retained for national security purposes

109. 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 chapter 1 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. The Counter-Terrorism and Border Security Act 2019 (the CTBS Act) made some changes to these retention periods, the impact of which is outlined at paragraphs 118-128 below.

110. The Protection of Freedoms Act 2012 (PoFA) sets out additional rules for the retention 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 deemed by a chief officer of police as representing a threat to national security). These rules apply to biometrics held by the police anywhere in the United Kingdom.

111. A responsible chief officer or chief constable[107] has the power to order that such biometrics be retained on the grounds that to do so is necessary in the interests of national security. The process by which they exercise this power is by making a National Security Determination (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. This power is unusual in that it is made by the police but is based entirely on an assessment of national security which is a matter for the Security Service. This necessarily requires very close partnership and cooperation.

112. An NSD must be in writing and lasts for a *maximum* of five years beginning with the date it is made.[108] An NSD may be renewed for a further period of up to five years and can be considered for renewal on any number of further occasions.

105 Similar provisions in Scotland are set out in the Criminal Procedure (Scotland) Act 1995.
106 TACT 2000, Schedule 8, paragraph 10.
107 (i.e. the Chief Officer or Chief Constable of the force or authority that 'owns' the biometric records at issue).
108 The statutory position as regards the period during which an NSD has effect in Northern Ireland is slightly different (see further Appendix C).

113. My function in relation to National Security Determinations (NSDs) is clearly set out in PoFA and is to keep under review:

(i) every NSD made or renewed;[109] and

(ii) the use to which biometric material so retained is put.

114. NSDs are made by chief officers of police and my role is not to 'approve' or consent to the NSD.[110] However, if I do not believe that retention of the relevant biometric material under the authority of the NSD is necessary then, in the absence of any other power under which the material might be lawfully retained, I may order its destruction.[111] This is a significant power which, given the threats being managed, I exercise carefully and not 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, as well as seeking assurance that the material is not otherwise capable of being lawfully retained. Of the 450 NSDs that I have reviewed since taking up office, I have not felt it necessary to exercise this power.

115. It should be noted that my duty to keep national security biometric retention and use under review only applies to material retained by police forces including British Transport Police, Ministry of Defence Police and armed services police such as the Royal Military Police; it does not to extend to any material that might be retained by non-law enforcement agencies, such as the security and intelligence services. There is a further category of 'law enforcement authorities' under PoFA[112] for these purposes and different agencies are empowered to have different access to the various biometrics databases used by the police.

Biometric databases for counter terrorism

116. The CT DNA Database is a standalone database of CT-related DNA profiles and crime scene stains. It is operated solely by the MPS's Secure Operations Forensic Services (SOFS). The CT Fingerprint Database is a separate and secure database within IDENT1 for CT-related fingerprints and crime scene finger-marks. The biometrics of individuals who are arrested, charged and/or convicted and who are deemed to represent a threat to national security 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 under the authority of an NSD will only be held on the CT biometric databases.

117. All DNA profiles loaded to the NDNAD are 'washed through' (compared 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 immigration and asylum fingerprints to be 'washed' through CT fingerprint databases. There are restrictions in place to ensure that only those with the relevant clearance, working in CT Command, are able to view the results of such searches.

109 It should be noted that the Scottish Biometrics Commissioner does not have functions in relation to NSDs and any matters pertaining to such determinations remains within the remit of the Commissioner for the Retention and Use of Biometric Material.

110 In contrast to the procedure by which chief police officers apply for retention of biometrics under s63G of the Police and Criminal Evidence Act 1984 as to which see paragraphs 78-104.

111 PoFA sections 20 (2) (a & b), (4) and (5).

112 See Parts I to VII of Schedule 1 to PoFA.

Legislative changes affecting NSDs

118. Following the terrorist attacks that took place in the UK in 2017 the then Prime Minister promised to bring forward further CT legislation. The legislation – the Counter-Terrorism and Border Security Act 2019 (the CTBS Act) – gained Royal Assent on 12 February 2019 and the relevant aspects of the legislation came into force on 13 August 2020. Alongside various provisions designed to support the police, law enforcement and intelligence agencies in combatting the threat posed by terrorism and hostile state activity, including the introduction of new powers for ports officers to stop and search people suspected of involvement in hostile activity (Schedule 3),[113] the Act amends the framework for making NSDs that was inserted into a range of other enactments by PoFA, specifically to:

    (i) Increase the maximum period of an NSD from two to five years.

    (ii) Allow any chief officer of a police force in England and Wales to make an NSD in respect of biometric material taken in England and Wales (rather than this being confined to a chief officer of the force which took the material).

    (iii) Allow multiple sets of fingerprints relating to the same individual to be retained under a single NSD (previously a new NSD, with a different expiry date, would have to be made in order to authorise the retention of any further sets of fingerprints taken from an individual whose fingerprints were already retained under an existing NSD).

119. The CTBS Act also introduced an automatic retention period of three years in a case where a person without a previous conviction is arrested under PACE on suspicion of a qualifying terrorism offence, to mirror the existing provision where a suspected terrorist is arrested under the Terrorism Act 2000 (TACT).

120. In his interim report[114] in December 2020 my predecessor outlined the teething problems that he had encountered in implementing this new legislation. I have similarly encountered some recurring issues with the approach taken by some chief officers when making NSDs which I outline in further detail below alongside several other initial observations.

121. First, my predecessor outlined in his interim report that, in anticipation of the new legislation coming into force, CT Command had added a new software patch to the form on which NSDs are made, which extended the 'default' retention period to 5 years rather than 2 years. Some NSDs made before the implementation date were recorded as having been authorised for 5 years and were therefore unlawful, although these errors have now been corrected so that all NSDs made before 13 August 2020 were for a maximum of 2 years. CT Command has since made clear that the previous erroneous recording of 5 years against these NSDs was a presentational issue rather than a practical one and did not impact upon the legal retention period referred to for review, renewal and destruction of biometric data.

122. Secondly, the CTBS Act extends the maximum retention period for an NSD from 2 to 5 years. The original PoFA retention period was a maximum of 2 years but because of the time taken to make an NSD decision and then prepare a case for a possible renewal,

113 Schedule 3 to the CTBS Act is modelled on the existing counter-terrorism powers at Schedule 7 to TACT and, similarly to those powers, provides for a chief officer to make an NSD authorising the retention of fingerprints and DNA profiles derived from samples taken under Schedule 3 (which must otherwise be deleted after six months).

114 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942155/Commissioner_for_the_retention_and_use_of_biometric_material_-_Interim_Report_December_2020__002_.pdf

virtually all NSDs were made for 2 years. A 5-year maximum however means that NSDs can and should be made for different lengths. A 5-year duration may be appropriate in cases where the risk presented by an individual is assessed not only to be significant, but also likely to continue for some time and allows police to review the situation at the appropriate intervals. In other cases, the risk being relied upon for the making of an NSD may be sufficiently evidenced to justify retaining the subject's biometrics but not yet certain or clear enough to justify a five-year retention period. In practice, this means that chief officers have to decide whether it is both necessary and proportionate to make an NSD in order to retain biometrics in the interests of national security **and** they have to determine a period of retention (up to the maximum of five years) that is necessary and proportionate having regard to the evidence before them.

123. It is already clear to me that some chief officers have followed this two-stage decision making process carefully and demonstrably while others have been less attentive in addressing the question of the appropriate length of time over which the NSD is to take effect. They have not been helped by the IT system used to process NSD casework defaulting to a 5-year retention period, an issue that was first raised with CT Command by my predecessor and which remains outstanding. I have adopted the same approach as my predecessor and challenged these NSDs where I do not believe that the information provided in support of the NSD fulfils the necessary requirements. The previous Commissioner wrote to chief officers in October 2020 to highlight this new requirement of a two-stage justification process. I am pleased that CT Command has issued, in January 2021, NSD guidance to assist chief officers and I have already seen a marked improvement in those NSDs that have been made since.

124. In previous Annual Reports my predecessor commented 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 is what has been referred to as 'pre-emptive NSDs'; because there is no need for an application since in either case the police could retain the biometrics at least until the investigative or legal processes were complete. The police reasoning for their doing so was that, if they decided to take no further action in an investigation and there was no other lawful basis for retaining the biometrics, the material 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.

125. The introduction in the CTBS Act of an automatic three-year retention period for biometrics taken from all those arrested on suspicion of a qualifying terrorist offence eliminates the need for many of these pre-emptive NSDs. Furthermore, the revised Statutory Guidance[115] on the making of NSDs allows the retention of biometric material for a further period of up to six months after an investigation into a non-terrorism related offence has ended to enable the police to consider or prepare an NSD. I have been advised that the practical changes required on PNC to prevent biometric material from being destroyed at the end

115 https://www.gov.uk/government/publications/national-security-determinations-that-allow-retention-of-biometric-data

of investigations in relevant cases where an NSD may be considered were implemented in autumn 2020. Since taking up post I have identified and challenged a small number of pre-emptive NSDs, though I expect these to decline in light of this legislative change.

126. A further helpful change to the NSD regime arising from the CTBS Act concerns the approving authority for NSDs. 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 or those forces covering a major airport or port) were experienced at making the necessary judgements while, in some other forces NSDs were very rarely needed and chief officers had little experience of making them or of the wider national security context in which NSDs are made. This produced some inevitable inconsistency in decision making. The CTBS Act has replaced the requirement and allows any chief officer to make an NSD.

127. It is CT Command's intention for each Regional Counter-Terrorism Unit to have a designated chief officer(s) who will consider NSDs. This should mean that NSDs will all be considered by a smaller group of experienced chief officers who will have a fuller understanding of the relevant issues and the context in which the threat assessed to be posed by the individual arises. Having reviewed over 450 NSDs during my first few months in post, this approach seems eminently sensible and should help achieve greater consistency in NSDs. I look forward to engaging with this group of chief officers once it is established later this year.

128. 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 was necessary in order to retain those biometric records. The new CT legislation changes this, by making an individual the object of an NSD rather than the material to be retained.

Section 18 Counter-Terrorism Act 2008

129. My predecessor has outlined in previous Annual Reports that CT Command had not brought the 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 made the subject of an NSD. The 2019 Annual Report reported that almost 300,000 fingerprint records were awaiting 'bulk deletion' due to them being held unlawfully (albeit in an unsearchable format). This was due to administrative issues and new governance put in place to avoid the inadvertent deletion of legally held material. Unfortunately, at the time of writing there are still 220,474 tenprint fingerprint records awaiting 'bulk deletion'. These records are not being held in a searchable format but are nevertheless being held unlawfully. The police and Home Office have assured me that they are working to rectify this as soon as possible and are looking at all options to determine the quickest route to complete the deletion of biometric material in accordance with the requirements of section 18 of the CTA. My office will continue to engage closely with Home Office and police stakeholders to keep me updated on progress to resolve this longstanding issue.

Use of the CT databases

130. At the commencement of the 'biometric' provisions of PoFA on 31 October 2013, the DNA profiles and/or fingerprints of 6,500 identified individuals were being held by police forces on the national CT databases. The comparable figure as at 31 December 2019 was 12,877[116] and as at 31 December 2020 was 12,676. 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 2020, 2099 (i.e. about 17%) of them have never been convicted of a recordable offence.

TABLE 18: Holdings of biometric material on the CT databases (year ending 31 December 2020)

		2019	2020
DNA	**DNA**	9,376	9,747
	Of which unconvicted	2,138 (23%)	2,143 (22%)
Fingerprints	**Fingerprints**	11,741	11,833
	Of which unconvicted	2,281 (19%)	1,939 (16%)
Totals	**Total holdings of material**	21,117	21,580
	Of which unconvicted	4,419 (21%)	4,082 (19%)
	Individuals on databases[117]	12,877[118]	12,676
	Of which unconvicted[119]	2,018 (23%)	2,099 (17%)

Source: SOFS

The NSD process

131. As explained above, deciding whether to make an NSD is a matter for chief officers of police.[120]

132. Initially, applications for NSDs are put together either by the MPS CT Command or PSNI. PSNI deals with all Northern Ireland cases but the MPS oversees all other cases and many of those are signed off by the CT Commander.

133. 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 overseas policing intelligence (if relevant) with additional supporting information from the Security Service. After recent terrorist incidents and the report by David Anderson QC,[121]

116 Figures supplied by SOFS for the 2019 Annual Report in relation to individuals with biometrics held on CT databases have been retrospectively corrected given that an erroneous method of data extraction was previously used.
117 Taking into account those with DNA and fingerprints held.
118 Please note figures supplied in the 2019 BC report (table 19), has been revised for 'Individual on database' to 12,877 of which 2476 are un convicted (19%), root cause of original data supplied attributed to wrong method of data extraction used.
119 Taking into account those with DNA and fingerprints held.
120 The term 'chief officer(s)' denotes both chief officer(s) and chief constable(s) of police forces, 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.
121 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

the Security Service re-examined their holding codes[122] (now referred to as "lifecycle status" categories) to ensure that they better reflect the residual risk of an individual as judged by the Service. While oversight of the Security Service is outside my remit I have met with them to discuss how a lifecycle status can help chief officers decide whether to make an NSD in relation to individuals, particularly where the only information available about an individual subject to an NSD application is held by the Service. As the codes are, in many cases, highly influential on the chief officers' decision to make an NSD, any effective oversight of that decision makes access to the background information essential and I will continue to engage with the Service on this matter.

134. If it is decided to make an NSD, the supporting information is summarised on the form. The NSD case present reasons as to why retention of biometrics is considered to be necessary on grounds of national security and whether such retention would be proportionate. CT 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 ultimately one for the chief officer, regardless of the advice offered, and they must record reasons for their decisions. The Statutory Guidance was updated and published in August 2020 on what should be considered following the changes made to the NSD regime by the CTBS Act discussed earlier in this chapter.[123]

135. The software for making NSDs runs on the police's National Secure Network to which I have access. When an NSD is made, 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 is available to me for review.

136. While I have challenged a number of cases where further information was required to justify retention of the associated biometric material, I am satisfied that the process followed complies with the legislation (including the Statutory Guidance). I anticipate that the elevated number of NSDs that were challenged in this reporting period and at the start of my tenure will decline as the legislative changes outlined bed in, and once the dedicated cadre of chief officers is established.

137. During 2020, the cases of 1,719 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 CT Command or PSNI for NSD purposes.

138. As can be seen in Table 19 (below), 406 NSDs were made by the CT Command and PSNI during 2020. My predecessor in his 2019 report outlined that (given that NSDs were limited to 2 years at this point) there was expected to be a bulge in renewal cases during 2020. Whilst there has been an increase, with renewals accounting for approximately 50% of all NSDs approved by chief officers in 2020 (compared to 29% in 2019), the caseload has been reduced by the COVID-19 pandemic and the effects of the Coronavirus Act 2020.

122 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.

123 See: Protection of Freedoms Act 2012: Revised guidance on the making and renewing of National Security Determinations allowing the retention of biometric data. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/908334/pfa2012-revised-guidance-making-renewing-national-security-determinations-retention-of-biometric-data.pdf

Section 24 Coronavirus Act

139. In March 2020, Parliament passed the Coronavirus Act 2020 in order to provide various emergency measures to help deal with the many and widespread contingencies of the COVID-19 pandemic. Section 24 of the Act empowered the Secretary of State to make regulations allowing the police to extend the statutory deadline for retaining fingerprints and DNA profiles by six months (with the option to extend this for a second occasion by a further six months, up to a maximum of 12 months in total) on grounds of national security in circumstances where there was no other lawful basis to retain these biometrics. This power allowed the police to retain the relevant biometrics without the requirement to carry out a detailed review of the risk posed by an individual and without the need for a chief officer to issue a National Security Determination (NSD) authorising retention.

140. My predecessor was consulted on the section 24 provisions at the time which he endorsed, noting that the police simply would not have had the resources necessary to make NSDs in the normal way given the unprecedented pressure on policing resources caused by the coronavirus pandemic.[124] Following CT Command's request to extend section 24 of the Coronavirus Act 2020 by six months, my predecessor provided a further report[125] on the use made of the power and attendant consequences before Parliament considered an extension for another six months. It was his view that circumstances had not materially changed since March 2020 in terms of the uncertainty around controlling infections and the associated disruption, but also that there was no evidence to suggest that the threats that the NSD regime is designed to deal with had diminished or were likely to do so in the following six months.

141. In this statement he further considered the interference in individuals rights involved in the use of section 24 and observed that CT Command continued to make some NSDs in the normal way as required by PoFA which he oversaw. It was only when resources or time limitations meant the police might lose biometrics that CT Command resorted to section 24. He therefore supported CT Command's request for a 6-month extension.

142. The second regulations came into effect on 1 October 2020 and expired on 24 March 2021 (though they continued to have effect beyond that on biometrics which would have otherwise expired before 24 March). Shortly after assuming post, I issued a statement[126] on the impact of the Act's measures over the full 12-month period from 2 April 2020 until 24 March 2021. During this period, 1,446 individual biometric profiles were subject to a section 24 6-month extension. Without the legislative intervention by the Home Secretary, these biometrics held by the police for reasons of national security would have been lost. I was also pleased to report that chief officers had continued to review and grant a significant number (over 300) of NSDs during the second half of the 12-month period, demonstrating that the section 24 power was used in a responsible and proportionate manner and only when scarcity of resources or time limitations meant that the biometrics of individuals assessed as presenting a real risk to national security might otherwise have been lost. In my statement, I referred to evidence that shows there is significant public support generally for a complete return to the systems protecting their rights before the exigencies of the

124 https://www.gov.uk/government/publications/biometrics-commissioners-response-to-coronavirus-bill-amendment/commissioners-response-to-coronavirus-bill-amendment
125 https://www.gov.uk/government/news/biometrics-commissioner-statement-on-the-coronavirus-act-and-the-protection-of-freedoms-act
126 https://www.gov.uk/government/publications/regulations-made-under-section-24-of-the-coronavirus-act-2020/biometrics-and-surveillance-camera-commissioner-statement-on-the-second-regulations-made-under-section-24-of-the-coronavirus-act-2020-accessible-vers

pandemic.[127] I am therefore encouraged by my second visit to CT Command (in April 2021) that the police and their partners in the NSD process have measures in place for a return to the established and enduring statutory process.

TABLE 19: NSD decisions (year ending 31st December 2020)

	2019	2020
Total possible NSDs applications processed	**1,374**	**1,719**
Renewal NSDs considered	262	154
New NSDs considered	1,112	1,565
NSDs approved by Chief Officer	**398**	**406**
Renewals	117	209
New NSDs	281	197
NSDs declined by Chief Officer	**25**	**11**
Renewals	7	5
New NSDs	18	6
NSDs supported by Commissioner	367[128]	155
NSDs challenged or further information sought	26	85
Destruction ordered by Commissioner	6	0

Source: SO15 and PSNI

143. My predecessor supported 155 of the NSDs made in 2020 and raised challenges in 85 (54%) of the cases examined. No NSDs were ordered for destruction in 2020. This is considerably higher than in 2019 when the Commissioner challenged only 7% of NSDs and largely reflects challenges my predecessor and I have made for those NSDs which do not evidence adequate consideration of the length over which the NSD is to have effect, particularly following the CTBS Act.

The use to which biometric material is put

144. I am required to keep under review the process of making NSDs and the use to which retained material is subsequently put. As can be seen in Table 20 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 potentially representing a threat to national security entering and leaving the UK using biometrics, regardless of what identity they may be using.

127 A recent survey by the Law Society found that two thirds of people said that after the pandemic it is important that people have the same ability to uphold their rights: https://www.lawgazette.co.uk/news/rule-of-law-should-not-take-a-backseat-in-pandemic-surveyfinds/5107728.article

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

TABLE 20: Matches with NSD retained material (year ending 31 December 2020)

Type of biometric match	Number of matches		
	2018	2019	2020
Fingerprint Crime Stain to Ten Prints	1	4	4
Ten print (Arrestee/Sched 7 etc) to Ten Prints	72	106	48
DNA Crime Stain to DNA Reference Profile	3	1	0
DNA Reference Profile to DNA Reference Profile	32	20	11
DNA Arrestee to DNA Reference Profile[129]	9	8	6

Source: SOFS and SO15

145. A dip sample has also been undertaken by the CT Command across 31 cases in this reporting period, where a newly taken biometric matched to NSD retained material. These cases equate to 65% of the total matches in 2020.[130] Some case studies have also been provided to me. Of particular note are the following:

- In one case, a DNA profile held under an NSD was matched to an unidentified CT crime scene stain in Spain. Home Office Immigration provided details that assisted Spanish authorities in formally identifying the suspect.
- Fingerprints on items recovered in conflict areas were matched to three subjects currently in the UK which resulted in investigations being opened.
- In several cases, a match to biometrics held under an NSD provided potential evidence related to wider criminal offences.
- In various cases, a match to biometrics held under an NSD provided intelligence to the police and others about overseas and other activities by the individual.
- In several cases, a match to biometrics held under an NSD confirmed the identity of individuals of terrorist concern that were operating under alias and opened up possible intervention opportunities for further disruptions.
- In one case, 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 was thereby prevented from entering the UK.

146. 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 2020, the police received over 500 'biometric notifications' against the CT fingerprint database in relation to asylum applications, visa applications and applications made for biometric residence permits. Having looked into these potential matches the police found that 16 individuals who had applied for asylum, 56 individuals who had applied for a biometric residence permit and 24 individuals who had applied for a visa had links to CT-related intelligence, with subsequent appropriate action being taken, including preventing individuals from entering the UK.

129 These are matches to material held under an NSD.
130 Compared with 2019 figures, there were around 50% fewer matches between newly taken biometric material obtained via Schedule 7 stops and NSD retained material in 2020, a result attributable to the significant reduction in overseas travel during the COVID-19 pandemic.

147. CT Command also manage the intelligence response to any matches made under the Prüm exchanges (see also Chapter 3) which may be linked to CT investigations. During 2020, there were 99 DNA and fingerprint matches to CT databases.

148. I appreciate the work undertaken by CT Command to provide my office with these case studies and data. Previous annual reports have outlined that routine tracking of every NSD case cannot be done using the current case management system and it is therefore not possible for me to provide the Home Secretary with detailed information on 'the use to which the biometric material is put' as required by PoFA . I am informed that CT Command will introduce a new IT system in the autumn of 2021 which will enable routine NSD case tracking, something which is clearly of as of much importance to their management of the terrorism risk as it is to my oversight role.

NSDs in Northern Ireland

149. The only assurance role that I fulfil in Northern Ireland is in relation to counter-terrorism holdings and the granting of National Security Determinations.

150. The Police Service of Northern Ireland Legacy Investigations Branch and Police Ombudsman have responsibility to investigate deaths in Northern Ireland related to the historic conflict. In 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.[131] This has been repeated on two further occasions, extending the period until 31 October 2022.[132] 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"*.[133]

151. 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 2022. If a further 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.

152. 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. My predecessor visited PSNI twice during 2019 and found them to be fully compliant in relation to material taken under counter-terrorism powers since the commencement of PoFA. I plan to follow this up with a further visit in the next year. 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

131 http://www.legislation.gov.uk/uksi/2016/682/contents/made
132 https://www.legislation.gov.uk/uksi/2020/688/contents/made
133 https://www.legislation.gov.uk/uksi/2016/682/pdfs/uksiem_20160682_en.pdf

arrangements outlined above.[134] At the time of writing the government is conducting a public consultation on a future strategy for addressing the complex legacy issues arising from Northern Ireland's past and I anticipate my office being asked to assist with some of the relevant biometrics considerations in the work that follows.

Data losses

153. 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. Fortunately, I can report that these issues have been resolved. As can be seen in Table 21 below, 144 biometrics were lost during 2018. This reduced to 4 in 2019 and, in 2020, only one set of biometrics was lost. CT Command has confirmed that this loss was due to an administrative error however, upon review, they would have not sought retention of this biometric material.

TABLE 21: Losses of biometric material of potential CT interest (year ending 31 December 2020)

Reason for loss of biometric data	Number of losses of biometric material		
	2018	2019	2020
Administrative error by SO15/SOFS	104	4	1
Case not reviewed by Chief Officer within statutory time limit	8	0	0
Case not progressed within statutory time limit	8	0	0
Taking of material not notified to SOFS	24	0	0

Source: SO15

134 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.

3. International exchanges of biometric material

154. Part of my role is to oversee the sharing of biometric material with international partners. It should be noted that this element is a specific sub-set of the much wider legal and regulatory framework governing the international processing of personal data generally. The international exchange of DNA profiles, fingerprints and associated demographic information is governed by the Home Office *International DNA and Fingerprint Exchange Policy for the United Kingdom*[135] which states that:

> *"The Biometrics 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."*

155. This policy clearly sets out the parameters in which DNA and fingerprint exchanges can take place and details the nationally agreed processes and mechanisms for doing so. When FIND-SB revised it to include both fingerprints and DNA[136] a distinction was made between the two, permitting fingerprints to be exchanged with biographical details at the outset. The only exception to this is Prüm exchanges which require biometrics and the associated personal data to be shared separately (discussed further at paras 183-193). In contrast, DNA exchanges are always anonymised until a match is established. As part of a wider update to the international exchange policy, the basis for this distinction will be reviewed by FINDS this year and I shall be involved in these discussions.

156. Since my predecessor issued the last annual report there have been various changes to the mechanisms used to exchange biometrics with the European partners owing to the UK leaving the EU on 31st December 2020. These changes will be discussed later in this chapter.

The role of the NCA, ACRO, the Counter-Terrorism Command and the ICCC

157. The National Crime Agency (NCA) has a coordination and liaison function as regards the exchange of biometric material between the UK and international law enforcement agencies. It deals with international fugitives, the case management of international enquiries and is the UK lead for extradition cases. 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.

158. ACRO is a national Criminal Records Office which is responsible to the National Police Chiefs' Council (NPCC). ACRO oversees the international exchange of criminal records and the loading of the foreign convictions to the PNC for:

- 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.

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

135 https://www.gov.uk/government/publications/international-dna-and-fingerprint-exchange-policy-for-the-uk
136 Previously the *International DNA Exchange Policy for the United Kingdom.*

160. The Metropolitan Police Service Counter-Terrorism Command also exchanges biometric information, as well as intelligence, with foreign powers. For example, they can share biometrically-enabled watch lists with partner countries. They also receive biometrics from overseas partners (usually in an anonymised form), which may then be retained on the UK CT biometric databases. 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.

161. 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.

Exchange of fingerprints and DNA for intelligence purposes

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

i. DNA samples

163. DNA samples (as opposed to profiles) are only exchanged in very rare situations where the subject consents. During 2020 there were no instances of DNA samples being exchanged with other countries.

ii. DNA profiles

164. DNA profiles are sometimes exchanged with other countries, though far less frequently than fingerprints. While fingerprints tend to be exchanged to confirm a subject's identity, a DNA profile is usually exchanged to try and identify 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 22 below provides the figures for inbound and outbound DNA Requests.

165. There are 4 types of DNA profile enquiry that are dealt with by the NCA:[137]

- *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 approval of the chief officer of the law enforcement agency that took the DNA sample and the Chair (or nominee of) 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.

137 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.

- *Outbound crime scene profiles and profiles from unidentified bodies*: Unidentified DNA profiles from crime scenes or from unidentified bodies/remains may be sent abroad for searching on another country's DNA database(s) at the request of the investigating police force. 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 offence committed would be a recordable offence carrying a sentence of more than a year's imprisonment under England and Wales legislation.[138] In every case consideration will be given to the question of whether or not "*the relevant exchanges and/or searches are necessary, reasonable and proportionate*".

TABLE 22: DNA INTERPOL profile enquiries (year ending 31 December 2020)

	Outbound from UK			Inbound to UK		
DNA Type	Total	Searches concluded[139]	Positive/ potential Match	Total	Searches concluded[140]	Positive/ potential Match
DNA samples	0	0	0	0	0	0
DNA subject profiles	30	26	2	38	21	1
DNA Missing persons	23	23	0	68	55	2
DNA crime scene profiles	104	94	14	272	18	38
DNA Unidentified bodies	141	141	16	165	162	34

Source: NCA

iii. Fingerprints and finger-marks

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

- *Outbound fingerprints*: This is the most common type of fingerprint exchange and usually takes place when 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 requesting fingerprints to be sent abroad must explain to the NCA why they think that there is a link to that specific country/ countries. The NCA also check the lawfulness, policing purpose, proportionality and safeguarding assessments prior to outbound exchange.

138 Or the equivalent in Scotland and Northern Ireland if it were committed in the UK.
139 Figures display the number of actual searches conducted (total number of searches minus rejected searches).

- *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.[140]

TABLE 23: Inbound and outbound fingerprint requests (year ending 31 December 2020)

	Outbound from UK			Inbound to UK		
Fingerprint Type	**Total**	**Searches concluded**	**Positive/ potential Match**	**Total**	**Searches concluded**	**Positive/ potential Match**
Ten Print Sets	328	Data not available	Data not available	1,355	Data not available	Data not available
Crime Scene Fingermarks	3	Data not available	Data not available	76	Data not available	Data not available

Source: NCA

167. Table 23 provides the figures for inbound and outbound fingerprint requests. Data on the number searches conducted and potential/positive matches has not been provided to me as the NCA do not systematically record this information owing to fingerprints being primarily used to confirm identity rather than establish links between crime scenes and known offenders.

iv. Dip sampling

168. My predecessors have visited the NCA annually and dip-sampled cases where an international biometric exchange took place, both for DNA and fingerprints, to ensure this is being done appropriately. This was not possible in 2020 due to the COVID-19 restrictions, alongside the political uncertainty about the terms of an UK-EU Agreement and whether international biometric exchanges with EU Member States would continue. I intend to resume these visits and will also carry out the first audit of the Prüm DNA and fingerprint exchanges together with the ICO and Forensic Science Regulator later this year (see also paragraph 186 below).

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

European Arrest Warrants

169. Prior to the UK leaving the EU on 31st December 2020, the NCA operated the UK SIRENE Bureau[141] which was responsible for managing the exchange of information relating to European Arrest Warrants (EAW) to assist law enforcement and border control. EAW requests were received from other EU Member States and often included the fingerprints of the relevant individuals. These fingerprints were loaded onto IDENT1 so that identity could be confirmed on arrest. It was a requirement that the fingerprints were deleted from IDENT1 at the end of the process (i.e. once a decision is made regarding extradition or the EAW is cancelled).

170. For outgoing EAW requests, fingerprints relating to the subject were sent to the country in question using the SIRENE system and were likewise deleted from the receiving country's database at the end of the process.

TABLE 24: EAW requests by fiscal year (2014/15 - 2019/20)

	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
Requests from the UK	223	241	345	296	146	185	324
Requests into the UK	12,134	14,279	16,598	17,256	15,540	14,553	15,939

Source: NCA

171. Table 24 provides a yearly comparison of the number of EAWs issued since 2014. During 2019/20, 269 individuals were arrested and 231 individuals surrendered as a result of EAW requests made by the UK. In the same period 1,086 individuals were arrested and 461 individuals surrendered as a result of EAW requests made to the UK.[142]

172. On 1st January 2021, the UK-EU Trade and Co-operation Agreement (TCA) introduced an arrest warrant to replace the EAW.[143] The SIRENE fingerprint collection is accordingly no longer available within PNC and all EAWs have reverted to the system previously used for Cyprus and Ireland (who did not use the SIRENE system) whereby fingerprints received are manually converted into the correct format, a dummy arrest summons created on PNC and the prints stored as part of the UK policing collection. This allows these fingerprints to be available for Livescan so that wanted subjects can be easily identified upon arrest. This is an interim measure whilst changes to the PNC and IDENT1 are considered with a view to establishing a quicker and more efficient system.

173. The NCA remains the central authority for certification of incoming extradition cases, arranging removals as well as the communication channel for extradition matters (via INTERPOL). The ICCC's National Extradition Unit (NEU) has been created this year to provide support and expertise to officers in England and Wales and will work closely the

141 SIRENE stands for Supplementary Information Request at the National Entries. Each member state which operates the Schengen Information System (SIS II) has a national SIRENE Bureau that is responsible for any supplementary information exchange and coordination of activities connected to SIS alerts (https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation_en).

142 Figures provided by the NCA.

143 Sections 12 and 13 of the European Union (Future Relationship) Act 2020 substituted any mention of the EAW Framework Decision in favour of the EU–UK Trade and Cooperation Agreement (TCA). See: https://www.legislation.gov.uk/ukpga/2020/29/enacted/data.htm Despite the change of name, the legislation still follows the Extradition Act 2003. See: https://www.legislation.gov.uk/ukpga/2003/41/contents

NCA, Police Scotland, PSNI, Immigration Enforcement, HMRC and a range of other law enforcement partners to target fugitives who have come to the UK as well as those fugitives wanted in the UK who are on the run internationally.

Exchanges of conviction information

174. The legal process under which the UK will notify EU Member States of convictions of their citizens in the UK is set out in Part 1 of the European Union (Future Relationship) Act 2020. During the reporting period covered by this annual report ACRO exchanged criminal conviction data with EU Member States under the former provisions[144] via the European Criminal Records Information Exchange System (ECRIS). This Framework requires an EU Member State convicting a national of another Member State to transmit information on the conviction to the country of the person's nationality.[145]

175. EU Member States can also 'request' conviction information where the national of another Member State is subject to criminal proceedings in order to find out whether they have convictions in their home country. This is done following the processes set out below.

i. Exchanges of fingerprints in the context of conviction information

176. 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 an EU 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 an 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 an EU 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 Member State. Sometimes that request will be accompanied by the subject's fingerprints.
- A 'Request In' may be received by ACRO from an EU Member State when a UK national comes to notice 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.

177. ACRO also exchanges conviction information and fingerprints with non-EU countries on behalf of the NCA and the Home Office. Those exchanges similarly take place in response to 'requests' and 'notifications' and may also involve the exchange of fingerprints.

178. Table 25 below provides comparative figures in relation to EU and non-EU exchange requests.

144 Under Framework Decision 2009/315/JHA.
145 There is no such legal requirement for non-EU countries.

TABLE 25: Fingerprint exchanges[146] (year ending 31 December 2020)

	EU Exchanges	Non-EU Exchanges
Requests in	568	1,474
Requests out	12,865	10,983
Notifications in	35	22
Notifications out	66,770[147]	13,745

Source: ACRO Criminal Records Office

179. It is clear from the above figures that a large amount of conviction and fingerprint data is shared between the UK and EU.

180. On 1st January 2021 the UK lost access to ECRIS, however the UK-EU TCA outlines that EU Member States may still use ECRIS technical infrastructure to co-operate with the UK on the exchange of criminal record data. The UK's Criminal Records Information System (UK-CRIS) has accordingly been set up to connect with Member States' software and exchange criminal record data. This exchange mechanism remains broadly the same as before EU Exit, although the timescales for sharing conviction information have changed. Under the TCA, notification of a conviction is communicated to the state of the convicted person's nationality once per month.[148] The new arrangements also set a time limit of 20 working days[149] for responses to a request for information, if for the purpose of criminal proceedings.[150] Whether this will have an operational impact on policing is yet to be seen.

ii. Loading non-UK convictions onto the PNC

181. Unless 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 connection with that conviction. Notably:

- there are strict limitations on how the UK can use conviction information about EU nationals obtained 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

146 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.
147 This number is significantly higher than previous years owing to a backlog of legacy notifications being sent to member states in autumn 2020 following a technical error affecting PNC records with dual nationalities or without a confirmed fingerprint status.
148 rather than 'as soon as possible' under ECRIS provisions.
149 previously 10 day under ECRIS.
150 126: Replies to requests, HM Government, Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, 24 December 2020.

- 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.[151] With few exceptions, 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.[152]

iii. UK nationals who have offended abroad

182. The convictions of UK nationals who have offended abroad are almost always recorded on the PNC whether or not they fall within the ambit of the list that is referred to above.[153] 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

183. The Prüm Council Decisions of 2008[154] 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.[155] Having initially opted out of a number of EU Justice and Home Affairs measures including Prüm in December 2015,[156] UK Parliament voted to opt in to Prüm on the basis that proposed safeguards would be brought into force. Those safeguards were agreed by Parliament and included the following conditions:

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

184. Since my predecessor's last report, the Home Office has conducted a review of its policy to exclude the DNA profiles and fingerprints of criminal suspects from Prüm exchanges. This was in response to a decision of the EU Council[157] which required the UK to "review its policy on the exchange of suspects' profiles". The Implementing Decision made it clear that the Council would "re-evaluate the situation with a view to the continuation or termination of DNA Prüm automated exchange" should they not be notified of the outcome of the review. My predecessor was consulted by the Home Office at the time and agreed in principle with the proposed policy but emphasised that any changes should be in line with data protection legislation and involve Parliamentary consultation.

151 See Appendix A. Also see *Commissioner for the Retention and Use of Biometric Material, Annual Report 2015* at paragraphs 76-78.
152 The exceptions are convictions in countries with which the UK has appropriate bilateral Agreements i.e. Albania, Anguilla, Antigua, Barbados, Cayman Islands, Ghana, Jamaica, Montserrat, St Kitts and Nevis, St Helena and Ascension Islands, Trinidad and Tobago, Turks and Caicos, United Arab Emirates, United States of America, Sovereign Base Area of Cyprus.
153 Convictions may, however, only be loaded to the PNC in respect of offences where there is an equivalent recordable offence in the UK.
154 2008/615/JHA and 2008/616/JHA
155 See also s.8 of the European Union (Future Relationship) Act 2020
156 See: http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm151208/debtext/151208-0002.htm#15120843000003.
157 Implementing Decision 2019/968. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0968

185. In June 2020, the Security Minister made a statement to Parliament confirming the Government's intention to begin exchanging suspects' data held in England & Wales and Northern Ireland with connected EU Member States through Prüm.[158] The Scottish Government also agreed to share suspects' data through Prüm.

186. Alongside the Information Commissioner, I have a role in overseeing and auditing the Prüm exchanges. The first full audit of the exchanges is due to take place in Autumn 2021. The FIND-SB also have a role in overseeing the exchanges as they involve the sharing of data held on the forensic information databases under its remit.

i. Prüm DNA

187. The Prüm DNA exchanges to/from the UK began to operate in July 2019 and the UK is now connected to 12 EU Member States[159]), representing over 80% of European DNA holdings. 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 Metropolitan Police Service, is the initial 'hit'/'no-hit' response.

TABLE 26: Prüm Step 1 DNA exchanges – UK matches (year ending 31 December 2020)

	Legacy hits	Business as usual hits
UK crime stain hits	1,347	3,141
UK subject hits	4,345	46,249

Source: Metropolitan Police Service[160]

188. 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.

189. 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.[161] Inbound Step 2 requests are those where there is a verified match against UK systems for a Member State and that State carries out a request to the NCA[162] for the associated demographic information.[163]

158 https://questions-statements.parliament.uk/written-statements/detail/2020-06-15/HCWS290
159 Austria, Germany, France, the Netherlands, Spain, Romania, Poland, the Czech Republic, Ireland, Latvia, Sweden and Belgium.
160 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.
161 All outbound requests are prioritised according to seriousness, urgency and capacity to respond.
162 This match is then scientifically validated by the UK before any request is processed.
163 All inbound requests are prioritised according to seriousness, urgency and capacity to respond.

TABLE 27: Prüm Step 2 DNA exchanges (year ending 31 December 2020)

	Outbound from the UK		Inbound to the UK	
	Total	Intelligence packages disseminated	Total	Intelligence packages disseminated
Step 2 hit with a person profile	831	662	1,821	1,773
Step 2 hit with a crime scene		169		48

Source: NCA[164]

190. It is clear from the above data that the exchanges of DNA profiles and unsolved crime stains that have taken place under this mechanism have yielded very significant results compared to the other EU exchange mechanisms. I am informed that previously unknown perpetrators of serious offences, including serious violent and sexual offences, have been identified through the Prüm mechanism. Fortunately, the UK continues to exchange DNA profiles with EU Member States under the UK-EU Trade and Co-operation Agreement. Further work remains to be done to promote the utility of Prüm at domestic police force level and encourage forces to follow up on Prüm matches. Information management processes to allow the tracking of the lifecycle of a Prüm case from a match through to a criminal justice outcome would provide valuable data against which the efficacy, necessity and proportionality of the Prüm arrangements could be assessed.

ii. Prüm Fingerprints

191. The UK connected with Germany in October 2020 and has since been exchanging fingerprints on a daily basis via Prüm. An automated feed permits the comparison of fingerprints (Step 1) and, once a hit occurs, the requestor verifies the hit and makes the request (Step 2) for the intelligence linked to the ten prints or crime mark.

TABLE 28: Prüm Step 1 fingerprint exchanges (year ending 31 December 2020)[165]

	Outbound
Searches requested	8,541
Hits	249

Source: MPS

192. In contrast to Prüm DNA, whereby DNA profiles are washed against a Member State's 'pot' (anonymised data) at the point of connection, Prüm fingerprints operates on a quota basis. Each participating State has a maximum daily quota of fingerprint searches against each other. These quotas are mutually agreed and are designed to limit the manual

164 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.

165 This data also includes searches during the period 1st - 6th January 2021. Data on the number of inbound searches requested/hits is not available.

resource required to verify matches. The Metropolitan Police Service has provided a manual 'gatekeeper' service to monitor daily quotas and initiate exchanges with Germany however this is a temporary solution. The NCA has developed and is currently trialling an automated gatekeeper which will allow multiple police forces to initiate requests without exceeding the daily quotas.

193. Table 29 below shows the number of outbound and inbound Prüm fingerprint Step 2 requests. The numbers are much smaller compared with DNA owing to the quota restrictions outlined above and the fact that the UK has only connected with Germany so far.

TABLE 29: Prüm Step 2 fingerprint exchanges (year ending 31 December 2020)

	Outbound from the UK		Inbound to the UK	
	Total	Searched concluded	Total	Searched concluded
Step 2 hit with a person profile	135	135	9	9
Step 2 hit with a crime scene		0		0

Appendix A

The biometric regime under PACE

1. The relevant statutory provisions introduced by the Protections of Freedoms Act 2012 (PoFA) inserted sections 63D to 63U and 65B of PACE and amended sections 65 and 65A.

DNA Samples

2. 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[166]

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 course action was to:

- treat the moment at which a decision is taken to take 'No Further Action' (NFA) against an arrestee as representing the 'conclusion' of the investigation of the relevant offence; and
- make the addition 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. The general rule set out in PoFA for DNA profiles and fingerprints is:

- they can continue to be kept indefinitely if the individual in question has been or is convicted of a recordable offence; but
- in almost all other circumstances they must be deleted from the national databases at the conclusion of the relevant investigation or proceedings.

166 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 any offence which is punishable with imprisonment[167] 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.[168]

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 paragraphs 6-7 of the main report.

Individuals arrested for Qualifying Offences

7. A 'qualifying' offence is, broadly speaking, a serious violent, sexual or terrorist offence or burglary.[169]

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 approves 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 to govern the retention and use of biometric material taken from young people under the age of 18 years.[170]

- 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'.

167 See section 118 of PACE.
168 See (new) section 65B of PACE and section 65 of the Crime and Disorder Act 1998.
169 See section 65A(2) of PACE.
170 See section 63K of PACE (as inserted by section 7 of PoFA).

- If a young person is convicted of a second recordable offence, their fingerprints and/or DNA profile may be retained indefinitely.

Penalty Notice for Disorder

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

Material retained for the purposes of National Security

11. Finally, PoFA 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.[171] In such cases biometric material may be held on the basis of an NSD for up to 5 years.[172] NSDs may be renewed before the date of their expiry for as many times as is deemed necessary and proportionate (see further **Appendix C)**.

Applications to District Judges (Magistrates' Court)

12. Where a person without previous convictions is charged with a qualifying offence or where the Biometrics Commissioner consents to an application under section 63G(2) or (3), by section 63F of PACE,[173] the resulting 3 year retention period may be extended for a further 2 years if, following an application by the relevant Chief Officer under section 63F(7), a District Judge so orders. The decision of the District Judge may be appealed to the Crown Court.

Convictions outside England and Wales

13. By section 70 of the Crime and Policing Act 2017, which amends sections 63F, 63H, 63I, 63J, 63K and 63N of PACE, the 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 only applies to biometrics taken in England and Wales on or after 03 April 2017.[174]

14. For those persons whose biometrics were taken by the police before 03 April 2017, by sections 61(6D), 62(2A) and 63(3E) of PACE[175] 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[176] 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

171 See sections 63M and 63U of PACE as inserted by sections 9 and 17 of PoFA) and Schedule 1 of PoFA.
172 The Counter-Terrorism and Border Security Act 2019 amended the maximum period of an NSD from 2 to 5 years.
173 (as inserted by section 3 of PoFA)
174 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. This is discussed further at paragraphs 47-48 in the main report.
175 (all inserted by section 3 Crime and Security Act 2010).
176 (inserted by section 6 PoFA)

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

Appendix B

Applications to the Biometrics and Surveillance Camera 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 A chief officer may make an application under section 63G(2) provided 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.[177] Whereas a chief officer may only make an application under section 63G(3) if they consider

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

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) 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 agree 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,[178] 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*"). As such, there is 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.[179] [In any event, unless an appropriate 'marker'[180] is placed on the PNC within 14 days of the making of an NFA entry, the biometric records of an individual without previous convictions who has been arrested for, but not charged with, a qualifying offence will automatically be deleted.]

Strategy Board Guidance and core principles

5. The Protection of Freedoms Act 2012 specifies that the National DNA Database Strategy Board[181] 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.[182] The Strategy Board endorsed the approach adopted by my predecessors for such applications and the

178 Further relevant provisions are at sections 63G(7) to (9).
179 There have continued to be some difficulties with this approach during 2020 as some forces have failed to update the PNC with the NFA outcome at the end of an investigation, although others have successfully addressed this problem since it was raised by my predecessor during earlier visits to police forces. The 63G application process 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.
180 As discussed in Chapter 1, UZ markers can be placed on PNC to prevent the automatic deletion of relevant biometric records if an application under section 63G has been or may be made.
181 Now known as the Forensic Information Databases Strategy Board.
182 See section 24 of PoFA which introduced (new) section 63AB(4) and (5) of PACE.

Board's detailed guidance issued in September 2013 was consistent with a document issued by the Commissioner at that time entitled *Principles for Assessing Applications for Biometric Retention.*

6. During 2018 a review was carried out of all casework practices and documents in relation to section 63G. As part of that review the two sets of 63G guidance were brought together into a single, revised document which was issued in September 2018 by the Strategy Board: https://www.gov.uk/government/publications/applications-to-the-biometrics-commissioner-under-pace

7. The key provisions of the guidance are as follows:

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

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

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

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

4. The Commissioner will require that the arrestee be informed of the reasons for any application and of the information upon which it is based. The reasons must be sufficiently detailed, so that the subject has a fair opportunity to make representations to the Biometrics Commissioner. If the arrestee is not so informed of any reasons or information which the applying officer seeks to rely upon, the Commissioner will attach no weight to them.

Relevant factors

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

(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.

OBSCC Documents

8. The Office of the Biometrics and Surveillance Commissioner has published a number of 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 Commissioner consents to an application under section 63G(2) or (3), by section 63F of PACE,[183] 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.[184]

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

Appendix C

National security provisions

Statutory background and guidance for 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 in accordance with other legislation, namely:

    - similar legislation applicable in Scotland and Northern Ireland; and
    - the Terrorism Act 2000 ('TACT'), the Counter-Terrorism Act 2008 ('the CTA'), the Terrorism Prevention and Investigation Measures Act 2011 ('the TPIMs Act') and the Counter-Terrorism and Border Security Act 2019 ('the CTBS 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 which govern the retention of biometric material by police forces anywhere in the United Kingdom which has been obtained from unconvicted individuals. 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 (NSD)'.[185]

4. An NSD is a determination made by a responsible chief officer or chief constable.[186] It must be in writing and, in England, Scotland and Wales, it has effect for a maximum of 5 years from the date it is made.[187] An NSD may be renewed before its expiry for a further period of 5 years.

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.

185 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 the report the word 'fingerprints' should be read as including 'relevant physical data' as so defined.

186 (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 following the provisions of the CTBS Act coming into force.

187 The CTBS Act extended the maximum period of an NSD from 2 to 5 years.

6. NSDs may be made or renewed under:

   (i) section 63M of the Police and Criminal Evidence Act 1984

   (ii) paragraph 20E of Schedule 8 to the Terrorism Act 2000

   (iii) section 18B of the Counter-Terrorism Act 2008

   (iv) paragraph 11 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011

   (v) section 18G of the Criminal Procedure (Scotland) Act 1995

   (vi) paragraph 7 of Schedule 1 to PoFA

   (vii) paragraph 46 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019.

7. The NSD process is primarily one for chief officers. 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 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. They must also disclose any information 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 which (revised in August 2020 prior to the CTBS Act coming into force) can be found at https://www.gov.uk/government/publications/national-security-determinations-that-allow-retention-of-biometric-data.

NSD Process

Applications for NSDs

12. NSD applications 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 an NSD, and their reasoned recommendation that the chief officer, chief constable or other responsible officer make or renew an NSD in the case at issue."*[188]

NDES/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:

> *"31. The chief officer, chief constable or other responsible officer 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; and*
>
> *(e) any other information considered relevant by the chief officer, chief constable or other responsible officer.*
>
> *32. The chief officer, chief constable or other responsible officer 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 (for example the risk that engagement by the subject in terrorism-related activity may go undetected) 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

188 See paragraph 41 of the Guidance. Paragraph 42 goes on to say *"… The application should set out all relevant factors and considerations including those which may undermine the case for making or renewing an NSD."*

authorities. In many cases it may also be appropriate for the chief officer to be provided with similar information about the individual's relevant associates and their activities and contacts with the authorities.

15. It is also expected, however, that chief officers will want to see more than a simple catalogue of historic facts and information about the individual and his or her associates. They will also want to be provided with a forward-looking analysis as to the nature of, and grounds for, existing and future concerns about the individual in question and with an explanation as to why it is believed that some genuinely useful purpose will be served by the retention of their DNA profile or fingerprints.

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.*"

This is a significant power which, given the threats being managed, requires careful use. In particular, it should not be exercised before the original decision has been challenged to ensure all the relevant matters have been taken into account by the chief officer and reflected in their reasons for making an NSD and assurances have been provided that the material is not otherwise capable of being lawfully retained. In practice, in reviewing the NSD the Commissioner is entirely reliant upon the information used by the chief officer in arriving at their determination (and therefore upon the information provided under the arrangements for review). The express further requirement for there to be no other means of lawful retention of the material before the power to order its destruction is

available requires the Commissioner to have considered all such other means and this will form part of the 'challenge' process that has been adopted between the police and the Commissioner's office.

The NSD IT System provides for the relevant challenges and final options available to the Commissioner It also assumes that the Commissioner will not take the second or third of those courses without first giving the relevant chief officer/NDES an opportunity to present further evidence and/or argument.

Retention and use of biometric material for national security purposes

DNA samples

20. 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.[189]

DNA profiles and fingerprints

21. 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).

22. Until 31 October 2013, 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[190] 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.[191] 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.

189 Section 20(8) Protection of Freedoms Act 2012. While Scotland has its own Biometrics Commissioner, the responsibility for CT and NSDs are not included in the statutory remit. See section 2(2) Scottish Biometrics Commissioner Act 2020.

190 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)

191 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)

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

Provision	Relevant material	Retention period[192]
Paragraph 20B Terrorism Act 2000 (TACT)	DNA profiles/fingerprints relating to persons detained under s.41 TACT.	3 years[193]
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.
Schedule 3, Paragraph 43 Counter Terrorism and Border Security Act 2019	DNA profiles/fingerprints relating to persons detained under sch.3 CTBSA.	6 months

192 The retention period starts from the date the relevant DNA sample/fingerprints were taken unless otherwise stated.
193 Since the CTBS Act has come into force, DNA profiles/fingerprints relating to persons arrested for terrorism offences under PACE are now subject to a 3 year retention period.

List of Acronyms

ACRO	ACRO Criminal Records Office
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
EAW	European Arrest Warrant
ECRIS	European Criminal Records Information Exchange System
FINDS	Forensic Information Databases Service
FINDS-DNA	Forensic Information Databases Service's DNA Unit
FIND-SB	Forensic Information Databases Strategy Board
FSPs	Forensic Service Providers
HOB	Home Office Biometrics Programme
IABS	Immigration and Asylum Biometric System
MPS	Metropolitan Police Service
NCA	National Crime Agency
NDES	National Digital Exploitation Service
NDNAD	National DNA Database
NFA	No Further Action
NLEDP	National Law Enforcement Data Programme
NPCC	National Police Chiefs' Council (which replaced the Association of Chief Police Officers ('ACPO')
NSD	National Security Determination
OBSCC	Office of the Biometrics and Surveillance Camera Commissioner
PACE	Police and Criminal Evidence Act 1984
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')
TACT	Terrorism Act 2000

TPIMs Act	Terrorism Prevention and Investigation Measures Act 2011
UKAS	United Kingdom Accreditation Service
UKICB	United Kingdom International Crime Bureau
UK-CRIS	United Kingdom Criminal Records Information System
UK-EU TCA	United Kingdom-European Union Trade and Co-operation Agreement

E02669527
978-1-5286-2890-7