Office of the Biometrics Commissioner

INTERIM REPORT BY THE COMMISSIONER FOR THE RETENTION AND USE OF BIOMETRIC MATERIAL

1. This short report is not a replacement for the Annual Report that the Biometrics Commissioner is required to make to the Home Secretary. My final Annual Report was submitted in March, and published in June this year, and it will be for my successor to present the next Annual Report. However, it seems to me unreasonable to expect a new Commissioner to provide detailed comments on events that happened under my watch and so I have produced this interim and my final report.

2. This report has been subject to a number of limitations. The most important of these is that due to the Covid-19 pandemic, we have not been able to carry out the normal regular visits to police forces as we have in the past. This means that I have much more limited first-hand experience to draw upon in preparing this report. In addition, the pandemic has disrupted many of the normal governance arrangements on which I have normally drawn in writing my Annual Report. This has also meant that I have been less able to respond to press enquiries about claims that may involve the police use of biometrics. I apologise for this but I do not comment without having clear information.

BIOMETRICS FOR LAW ENFORCEMENT IN ENGLAND & WALES

PoFA Regulation of the Police Use of Biometrics

3. A general description of the regulation under the Protection of Freedoms Act 2012 (PoFA) of the police taking, retention and use of DNA and fingerprints can be found in the Commissioner's Annual Reports[1]. The purpose of this interim report is not to provide the detailed descriptions and statistics about all the processes involved since that will be provided

[1]The latest of which can be found at: https:assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

later in the Annual Report, but instead to draw attention to any issues that I am aware of. These are inevitably limited for the reasons given above.

Biometrics and New Policing Programmes

4. One issue that has arisen concerns how the PoFA rules apply to some innovative policing programmes. Many forces have programmes, sometimes experimental, to deal with minor crimes, especially by juveniles, using community disposals in order to reduce the risk of re-enforcing criminality. This has raised the question as to whether biometrics can be taken and whether in such cases an application to the Commissioner for the retention of such biometrics under Section 63G of the Police and Criminal Evidence Act as amended (PACE) is possible if there is no other lawful basis for retention. The answer, of course, depends on the detailed nature of each scheme, including the suspected offence.

5. The Forensic Information Databases Strategy Board (FINDS-SB)[2] has agreed to look into the various schemes currently in operation and then provide advice to forces. I am grateful to Assistant Chief Constable Ben Snuggs, the Chair of FINDS-SB, for agreeing to take on this task.

The CPIA Exception

6. Previous Annual Reports have discussed the possible tension between the requirements of PoFA and that of the Criminal Procedure and Investigation Act 1996 (CPIA). Put briefly, PoFA requires that DNA samples should be destroyed either once a DNA profile has been derived from them, or after 6 months. This is to guard against the use of a DNA sample to gain information other than that needed for a criminal investigation and was a new protection introduced by PoFA. When PoFA came into force, the police had to destroy the large number of DNA samples that they were holding under previous legislation.

[2] FINDS-SB is a statutory Board set up by PoFA (originally called the DNA Strategy Board).

7. The CPIA, however, allows DNA samples to be retained until a criminal investigation and allied disclosure arrangements are concluded. If the CPIA exception were to be liberally applied, then it would seriously undermine the PoFA rules on the retention and deletion of DNA samples. It is possible for forces to take different views on the circumstances under which a DNA sample may be retained under the CPIA exception and indeed they do so.

8. My predecessor suggested some years ago that either the Home Office or the police ought to issue guidance on the circumstances under which it was reasonable to keep DNA samples in such a way as to retain the integrity of the PoFA rules and ministers agreed with this in 2016. When this did not happen, I wrote to all forces in December 2017 setting out my concerns and suggesting principles for the use of the CPIA exception - a copy of that letter is attached as an appendix. I regarded that as an interim measure until proper guidance could be issued. I regret that I have to report yet again that such guidance has not been issued.

9. As a result of the Covid-19 pandemic we have not visited police forces since my last Annual Report was published but I did write to all forces seeking basic data on a number of issues, one of which was their use of the CPIA exception. The data we have recently received shows that there is still significant variation in the extent to which forces are using the CPIA exception to retain DNA samples that they would not otherwise be able to retain under the PoFA rules. Some forces are clearly not following the principles that I suggested in my letter to all Chief Constables in 2017.

10. This problem was identified fairly quickly and probably should have been predicted in advance. Yet the need for guidance has still not been addressed. Let me be clear, there are criminal investigations where it is reasonable and lawful to retain DNA samples in the interests of justice. My concern is the public need to be reassured that this is done in a similar way by different police forces: that there is not a postcode lottery in the application of the protections introduced by PoFA. Issuing guidance would provide that assurance and it is now four years since ministers committed to do so.

The Taking of Biometrics by the Police

11. My reporting, as Commissioner, has been concerned with whether the police are implementing the protections built into PoFA, but I have also reported on the importance for criminal investigations of the taking of biometrics in order to keep the public safe from crime. There has been a problem, over recent years, that the number of DNA profiles and fingerprints added to the national databases has declined. Whilst I have suggested that the increasing use of voluntary attendance, rather than arrests, has been one reason, Home Office policing researchers in a presentation to FINDS-SB argued that other factors must also have been involved. Irrespective of why the decline has happened, the utility of the police use of biometrics will be undermined if the police do not take and retain those biometrics that they are entitled to under the legislation.

12. Since this has been a growing concern, I was interested to find out whether the Covid-19 pandemic had had any effect on the taking of biometric samples. I therefore asked all police forces in England & Wales to provide me with some basic information in this regard.

13. When it became clear that the pandemic might have an effect on normal policing operations, the Forensic Capability Network drew up some guidance to try and protect the taking of biometrics both from arrestees and at crime scenes. This guidance was subsequently endorsed by the NPCC portfolio lead for fingerprints, Chief Constable Rachel Swann. The evidence that we have received shows that this guidance has been largely successful. There was a fall in the taking of biometrics initially as forces adjusted to the immediate effects of the pandemic, but more long-term most forces have retained their earlier level of adding new biometrics to the national databases. There were some changes, for example some reduction in the taking of repeat fingerprints or the upgrading of DNA profiles but not to a worrying degree. Some forces saw a drop in the taking of biometrics simply because of a fall in the number of arrests, as was the case for British Transport Police reflecting the fall in train travel caused by the pandemic and the restrictions imposed in response. One exception to this general picture, is that it remains the case that some forces are still taking few biometrics from voluntary attendees when it was

lawful to do so, especially where their IT systems do not facilitate this taking. However, this is not a consequence of the pandemic but a problem for which the origins lie elsewhere and was discussed in my last Annual Report.[3]

The Legality of the Police use of New Biometrics

14. The legality of the police deployment of new biometrics, beyond those regulated by PoFA, was contested as soon as South Wales Police (SWP) began the first Home Office-funded trial of the use of live automated facial recognition (AFR). *Liberty* challenged the legality of the use of AFR by South Wales Police and *Big Brother Watch* threatened to challenge similar use of AFR by the Metropolitan Police.

15. In the event it was *Liberty's* challenge, on behalf of Mr Edward Bridges, against SWP that was the first to come to court. The Surveillance Camera Commissioner also joined the action to test whether the use of AFR met the requirements of the Home Secretary's Surveillance Camera Code of Practice which provides guidance on the overt[4] use of public facing camera systems. The action was also joined by the Information Commissioner to test whether the police use of AFR met the requirements of the Data Protection Act 2018, under which she has specific statutory powers.

16. The case was heard by the High Court in Cardiff in September 2019 which decided that the way in which SWP had used AFR was lawful. I commented on that judgment at the time.[5]

17. The parties to that action subsequently appealed the decision of the High Court. The Appeal Court's judgment was handed down on the 11th

---

[3] See paras 125-133 of https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

[4] None of the parties challenged the legal basis of the covert use of these system since that is governed by separate legislation.

[5] https://www.gov.uk/government/news/automated-facial-recognition

August 2020[6]. The Appeal Court overturned the earlier decision and held that SWP had not met the necessary tests of legality in their use of AFR.

18. The Court commented that:

> "*The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the 'who question' at the hearing before us. The second is the 'where question'. In relation to both those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on a watch list nor is it clear that there are criteria for determining where AFR can be deployed" (91*).

19. The Court continued that the policies currently in place were not detailed enough to enable the police to overcome this deficiency. It is not, of course, for the courts to decide what such policies should be, but the Court did suggest that even if local policies were to exist, it would be 'prudent' to have national consistency, perhaps via the Secretary of State's Surveillance Camera Code of Practice.

20. To address the absence of national policy as regards these two issues the Home Office have set up a group chaired by Jeremy Vaughan, Chief Constable of SWP and NPCC lead on facial matching, to create national guidelines for the use of facial matching by police in England & Wales. If that is successful, it might be held to deal with the concerns of the Appeal Court.

21. Having ruled that the use of AFR by SWP was unlawful because it failed to adequately deal with the questions of watch lists and where AFR can be deployed, the Appeal Court did not address the question of whether, if it had been lawful, it would have been proportionate. If the police and Home Office develop guidelines for any future deployment of AFR to meet a legality test, then they will also have to pay regard as to whether they can be justified as proportionate.

---

[6] [2020] EWCA Civ 1058

22. The Appeal Court then turned to whether SWP had adequately carried out a Data Protection Impact Assessment before deploying AFR. The Equality Act 2010 places a positive and ongoing duty on the police (and other bodies) to have due regard to eliminate any discrimination in the use of AFR against those with protected characteristics - what is called the Public Service Equality Duty (PSED). The Court said:

    "The two protected characteristics that are relevant in the present case are race and sex. - - - It is said that there is scientific evidence that facial recognition software can be biased and create a greater risk of false identification in the case of people from black, Asian and other minority ethnic ("BAME") backgrounds, and also in the case of women." (164)

23. The Appeal Court held that:

    "The fact remains, however, that SWP have never sought to satisfy themselves either directly or by way of independent verification, that the software programme in this case does not have an unacceptable bias on grounds of race or sex." (199). And therefore

    "In all the circumstances, therefore, we have reached the conclusion that SWP have not done all that they reasonably could to fulfil the PSED. We would hope that as AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias." (201)

24. The Court stressed that the PSED is a duty of process not outcome. As quoted above, the judgment makes clear that the PSED test is met if the police have done everything that they reasonably can to understand any bias in the software that they are using or in the manner in which it is being used. That is important since in the SWP case the vendor of the software they used refused to release details of their software on grounds of commercial confidentiality. That, in itself, is not fatal to meeting the PSED test, although the police may prefer to work with vendors who will

help them fulfil their duty in this regard. In my view, it is not bias itself that is fatal to legality. Rather it is not ensuring that any bias is understood and action taken to mitigate the effect in deployment, or, if that is not possible, not to use the algorithm in question.

25. The relative quality of facial matching software has been independently examined by the US *National Institute of Standards & Technology* (NIST), for those vendors who have submitted their software for evaluation[7] and they have specifically examined the question of bias in relation to protected characteristics[8]. These tests will be useful for police forces contemplating any future use of AFR, since they test for positive and negative bias in both one-to-one verification and one-to-many matching tasks,are of a good scientific standard and independent of the vendors of the software. The database upon which a vendor's software has been trained is one possible source of bias and NIST testing shows some unexpected differences between different algorithms in this regard. Most vendors are well aware of the bias problem and some are reportedly examining the use of a number of different, more localised demographic training databases for different markets.

26. Like any scientific evaluation, NIST testing still has limitations. Essentially this comes down to the fact that an English or Welsh police force will want to try and understand any bias of the software that they are planning to use in relation to the demographic profile of the population of England & Wales, or ideally, that of the population in their force area. NIST tests for biases in algorithms against a library of facial images gathered by US government agencies but, of course, that library does not necessarily reflect UK demographics. Furthermore, NIST is conducting lab-based tests which may be different to real world deployment testing. Notwithstanding these limitations, Dr Patrick Grother, the lead NIST test scientist, rightly in my view concluded:

---

[7] see:https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software Vendors volunteer their software for testing but on the understanding that the results will be published. Most major vendors have done so, including recently some of the software developed by the global tech companies. Users can draw their own conclusions from software that is not offered for testing.

[8] see:https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

"While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied." and "While we do not explore what might cause these differentials, this data will be valuable to policymakers, developers and end users in thinking about the limitations and appropriate use of these algorithms."

27. NIST testing is certainly useful to help UK police forces demonstrate they have met the PSED but unless bias in algorithms is removed, or more realistically significantly reduced, police forces would be advised to do what they can to carry out pre-deployment trials and continue to monitor as best they can bias in a local deployment context. In this regard, it would be helpful if the NPCC drew up national standards for police trials and ongoing monitoring of the use of AFR. The NPCC is about to appoint a Chief Scientific Advisor and that should provide a focus for this and similar work on other new police technologies.[9]

28. To fully meet the PSED obligations, forces will have to consider any discriminatory effects of the algorithms that they are proposing to use and whether any such possible effects will exacerbate any discrimination that may have taken place prior to the deployment of the software. For example, if there is evidence that there may be discrimination in a police force's use of their arrest powers, then that may feed through to the database from which a watch list is drawn up for use in an AFR deployment. If the protected characteristic which had been discriminated against in the exercise of arrest powers was the same characteristic that the evidence suggested was discriminated against by the AFR software, then that would have a compounding discriminatory effect or vice versa. This is simply to recognise that any discrimination in the criminal justice system cannot be examined as an isolated event but instead for its systemic consequences.

[9] I commented in my evidence before the Select Committee for Science & Technology that there was a discrepancy between the police use of the term "trial' and the normal scientific use of the word and that was not merely a verbal quibble but an important issue about what counted as evidence in addressing the kind of questions raised by the Appeal Court.

29. The Appeal Court judgement does not prevent future police use of AFR for, as my colleague the Surveillance Camera Commissioner, Tony Porter said at the time of the Bridges judgment:

> *"I very much welcome the findings of the court in these circumstances. I do not believe the judgment is fatal to the use of this technology, indeed, I believe adoption of new and advancing technologies is an important element of keeping citizens safe. It does however set clear parameters as to use, regulation and legal oversight."*

I agree with that comment. The Appeal Court judgement was about the legality of the use by the police of AFR and specifically about the use by SWP. It was not about the use of AFR by other forces, such as the Metropolitan Police, nor about police use of other new biometrics or other AI-driven technologies. However, the issues that the Court drew attention to in regard to SWP's use of AFR will clearly need to be properly addressed by any further police use of AFR in order for this to be lawful. The general principles which the Court pointed to would also need to be considered before the use of AFR by any other body, public or private. Any use of other new biometrics or other AI-driven technologies that share similar characteristics to the police use of AFR (matching by algorithm against a watch list drawn from a database by using some form of general public surveillance) will also raise similar issues.

30. There are limitations to the role of the Courts in determining the legality of the use of the rapidly growing new AI algorithm-driven technologies. The Appeal Court was careful to point out that it was not its job to create policy but to interpret the law, however, at the same time pointed to the inadequacies of current policy in relation to AFR. For that reason, I continue to believe that not only new policy, but also new legislation that regulates the police use of new biometrics, is needed. Having argued that case in my recently published Annual Report, I do not intend to rehearse the arguments again as to why that is the case.[10] The work by the police and the Home Office to draw up guidelines for the use of facial matching is welcome, but this technology is surely important enough in

[10] https:assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

terms of its implications for us all that policy for its use ought to be decided by Parliament and not by those who may have a vested interest interest in how new technology is used. That is not to cast aspersions on the motives of either the police or ministers. Indeed, in my experience the police are very aware of the need to balance the interests of law enforcement with individual liberties. Instead it is simply a matter of good governance in a democracy.

BIOMETRICS AND NATIONAL SECURITY

The Duties of the Commissioner as Regards National Security

31. Under the Protection of Freedoms Act 2012, the Biometrics Commissioner has two obligations in relation to the use of biometrics for purposes of national security. They are to keep under review:

> *(i) every National Security Determination (NSD) made or renewed, and*
>
> *(ii) the use to which the biometric material retained is being put.*

32. The first of these requirements goes together with the Commissioner having the power to order the deletion of biometrics if an NSD is judged not to have been properly made. Reviewing all NSDs has been a significant part of my workload[11] but neither myself nor my predecessor have had any trouble in fulfilling this first requirement to review NSDs.

33. The second of the obligations, however, has remained problematic. This is because the software used by CT Policing for the making of NSDs was not designed to make analysis easy nor does it link easily to other information sources. The result is that I have not been able to supply to the Home Secretary and thence Parliament the kind of analysis to a satisfactory level that the legislation envisaged. Instead, CT Policing have supplied me with limited case studies or very small samples of data which I have reported on in my Annual Reports but this has not been

[11] This should now reduce over time with the change to allowing NSDs to be made for a maximum of 5 rather 2 years - see below.

adequate. CT Policing commissioned new software some time ago that will include an analytic capability, but this has still not been put in place.

34. This is worrying for two reasons. First, maintaining the NSD process is a costly business and we need to know that the money is well spent compared with alternative uses. Secondly, I would have expected Counter-Terrorism Command to want to use data analytics to examine whether NSDs can be used to improve its grip on the terrorism risks.

35. I hope that by the time my successor comes to write an Annual Report, the means will be available so that they can fulfil this second aspect of their legislative mandate.

Third Party Access to Police Databases

36. At the time of writing my last Annual Report there was the outstanding issue of whether the Ministry of Defence (MoD) should be allowed to have access to the police National Fingerprint Database. I have commented on this issue in several Annual Reports, including the most recent.[12]

37. Shortly after my last Annual Report was written, the NPCC received legal advice on whether there was a lawful basis for the MoD accessing the National Fingerprint Database. The Chief Constables, collectively, are the data owners of the national fingerprint database and as such they can decide whether they will allow third party access. The legal advice provided to the NPCC was that the MoD, in running their CT biometric data holdings against the police National Fingerprint Database for possible matches, were not doing so in a way that raised the issue of whether there was a legal impediment to them doing so. The NPCC have therefore agreed to allow the MoD's use of the National Fingerprint Database to continue. Any risk, therefore, now sits with the Chief Constables.

[12] see paras242-248 of https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

38. This does, however, raise two questions. First, do the Chief Constables, as the data owners, have an unfettered right to allow others to have access to national policing databases? Certainly, a number of organisations have been granted some access to police custody facial images stored on the Police National Database. These have largely been agencies who are involved in some kind of rule enforcement, although not necessarily policing bodies as defined in PoFA. That raises the second question of whether the Chief Constables are answerable in any public way for such decisions. It is certainly not easy to discover who has been granted access to policing databases.

39. In addition to the narrow question of who has access to police databases, there is the much broader question of who has access to all databases belonging to government or its agencies. The public are already sceptical about who commercial companies share their data with. However, when state agencies collect our data, sometimes under legal mandate, surely we ought to know not only what it is being used for but who it will be shared with and for what purpose? Such activity is regulated by the Information Commissioner under the Data Protection Act but that is a backstop for the transparency we might expect in a democracy. Data analytics and data sharing undoubtedly will provide benefits that serve the public interest, but some may not and enabling those benefits will depend on public trust. We have seen during the pandemic how distrustful some of the public have been about the data use and subsequent data sharing of the NHS Covid-19 Test and Trace App. The government needs to think about how it will create public trust, what data sharing is acceptable to the public and how that should be regulated.

New Counter-Terrorism Legislation

40. In 2019 the Counter-Terrorism and Border Security Act was passed. The aspect of the legislation that affected Chief Officers making National Security Determinations (NSDs), in order to retain DNA profiles and/or fingerprints, was explored in my last Annual Report[13]. The relevant

[13] See paras 230-237 of https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

aspects of the legislation came into force on 13th August 2020 and at the same time the Home Office published guidance[14].

41. As so often happens when new legislation comes into force, there have been a few teething problems with its implementation.

42. The Protection of Freedoms Act 2012 allowed Chief Officers of Police to make an NSD if they judged that it was necessary and proportionate to retain a person's biometrics for national security purposes in circumstances where there was no other legal basis for doing so. If an NSD was made, then it remained in force for a maximum of 2 years but could then be renewed on any number of occasions. The new Act extends this period for retaining biometrics under an NSD to a maximum of 5 years. Two problems have so far occurred in implementing this new provision.

43. First, in anticipation of the new legislation coming into force CT Policing 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. Unfortunately, this patch became active before the implementation date of 13th August 2020. During my routine oversight of NSDs, I noticed that some NSDs made before the implementation date were recorded as having been authorised for 5 years and were unlawful, although the Chief Officers making the NSDs were not necessarily aware of this because it was an automatic default. I raised the problem with CT Policing and I have been assured that all these errors have now been corrected so that NSDs made before 13th August 2020 were for a maximum of 2 years.

44. Secondly, the Act extended 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 extension, virtually all NSDs were in reality made for 2 years. However, a 5-year *maximum* means that NSDs can now realistically be made for different lengths. In practice this means that

[14] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/908335/pfa2012-revised-guidance-making-renewing-national-security-determinations-retention-of-biometric-data-print.pdf

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 what period of retention (up to *maximum* of 5 years) is necessary and proportionate having regard to the evidence before them. In my routine oversight of NSDs after the new 5 year maximum came into force, I found that some Chief Officers were following this two-stage decision making process and authorising NSDs of different lengths, but others were not addressing the question of the length of the NSD and the software was then making them for 5 years by default. I challenged all these later NSDs as not fulfilling the necessary considerations.

45. CT Policing was planning to issue their own guidance for the making of NSDs in light of the new legislation, but this had not happened when the changes came into force. As an interim measure, I therefore wrote to all Chief Constables in the UK explaining my view that the length of retention should be considered and justified in making an NSD. I have also raised my concern that setting the 5-year maximum as the default length on the NSD form doesn't encourage Chief Officers to think about the appropriate length of retention.

46. At the same time as the Counter-Terrorism and Border Security Act came into force, the British Security Service (MI5 or the 'Security Service') also introduced a new system for categorising the relative risks of those known to the Service as possible threats to national security. The new system is intended to be a finer-grained risk assessment which is reviewed more regularly in order to help guide the Service's operations. The new system was also a response to some criticisms made by a official review of some recent terrorist attacks.[15] This is relevant to the making of NSDs, since the assessments presented to chief officers include the risk assessment of the subject by the Security Service. In the past such assessments were only available for some (often a minority) of applications in which the Service was actively interested. However, the new system will provide a risk assessment for all those the Service is aware of as posing, or having posed, a possible risk and that may apply to a larger group of NSD

[15] David Anderson: *Attacks In London and Manchester, March-June 2017*
Independent Assessment of MI5 and Police Internal Reviews, Unclassified, December 2007

applications. These risk assessments are useful in deciding an NSD application, but the Chief Officer may only be given the category of risk and a generic description of what kind of risks fall into that category. Where there is sufficient evidence of an adequate quality from other sources for a Chief Officer to consider, then any lack of detail of what lies behind the Security Service's risk assessment may not be a problem. However, where the decision on an NSD hinges on the Security Service's risk assessment, the Chief Officer will need to know more about what lies behind the Service's assessment since deciding whether to make an NSD lies, in law, with a Chief Officer of police exercising their mind on the evidence before them.

The Future for CT Policing

47. In my last Annual Report I discussed the future of CT Policing and said:

> *"As is alluded to in this chapter the police Counter-Terrorism Command are working increasingly closely with the MoD and the Security Service. Representatives of both these bodies attend the National Security Biometrics Board, which is sensible given that this reflects current practice. Slightly at odds with this, however, is the current legislative regime as set out in PoFA, which at the time it was drafted essentially envisaged the police being solely responsible for the collection, retention and use of DNA and fingerprints for domestic national security purposes. Furthermore, facial image collection, retention and use for the purposes of national security is now routine but is not governed by PoFA. This raises an important question, particularly in light of the government's manifesto commitment to legislate in this area. For the future – does Parliament wish to re-assert the primacy of the police in domestic national security capture, retention and use of biometrics or instead does it want to legislate to cover the roles of the police, the Security Service and the MoD in their use of biometrics for domestic national security? The choice has implications for how far the Counter-Terrorism Command remain closely linked to the rest of policing or become rather separate and more closely linked to the Security Service and the MoD. It also has*

implications for how the future governance of the use of biometrics for national security should be structured."[16]

48. In October 2019, the government announced an Integrated Review of Security, Defence, Foreign Policy and Development that might answer some of these issues, but its publication has been delayed by the Covid-19 pandemic. However, the Spending Review 2020 seemed to prefigure some likely outcomes of the Review as it provided the UK Intelligence Community (UKIC) with a £173 million funding increase in 2021-22, representing a 5.4 per cent average annual real-terms increase since 2019-20. Some of that was to fund:

"*The delivery of a world-leading new Counter-Terrorism Operations Centre. This will bring UKIC (UK Intelligence Community), counter-terrorism policing and other parts of the criminal justice system together into one location. This new, fully integrated approach will keep the public safer from terrorism by enhancing the ability to discover and prevent attacks, improve the speed of response, and work together more efficiently."*[17]

49. Increased cooperation is to be welcomed, because limited co-operation and sharing of intelligence information has been criticised by post-hoc reviews of some recent terrorist attacks. There is a risk, however, that if CT Policing and related parts of the criminal justice system work more closely with the security and intelligence agencies and the MoD, they could become less connected with the rest of policing and the link to on-the-street policing knowledge and intelligence so crucial for terrorism prevention and investigation.

The Effects of the Covid-19 pandemic on the Making of NSDs

50. In March 2020, Parliament passed the Coronavirus Act in order to provide various emergency measures to help deal with the Covid-19 pandemic.

---

[16] See Para 270https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897090/Biometrics_Commissioner_Annual_Report_Web_Access.pdf

[17] See: https://www.gov.uk/government/publications/spending-review-2020-documents/spending-review-2020#strengthening-the-uks-place-in-the-world-1

Section 24 of the Act enabled the Home Secretary to make regulations allowing the police to keep fingerprints and DNA profiles for six months on grounds of national security when there was no other statutory basis for keeping these biometrics. The police can do so without carrying out a detailed review of the risk posed by an individual or the making of an NSD by a Chief Officer as would normally happen. .

51. Before this provision was put before Parliament, the Minister for National Security sought my views as to whether such provision was necessary. At the time I thought that the impact of the pandemic on the ability of the police to make NSDs in the normal way was uncertain and that carried a risk that biometrics of national security importance could be lost. I laid out and published my views at the time and before Parliament considered Section 24 of the Coronavirus Act[18].

52. The Coronavirus Act was emergency legislation to deal with an immediate crisis, but its passing was not without controversy. One change that Parliament insisted on, was that any further extension of the Act, beyond its initial six months, would have to be agreed by Parliament rather by delegated authority. Furthermore, a second six-month period would be the maximum permitted.

53. Towards the end of this initial six-month period, CT Policing made a formal request to the Home Office for a six-month extension to Section 24. I was again consulted and again made a public statement as to my view before Parliament considered the matter and also provided statistical information as to what use had been made of Section 24.[19] Whilst I thought that ongoing uncertainties about the Covid-19 pandemic justified the further extension of Section 24, I also pointed out:

"The power originally granted by the Protection of Freedoms Act 2012 (PoFA) to allow chief officers of police to make NSDs was a significant one. It allows for the keeping of biometrics for national security reasons where no other statutory power to do so exists and where the subject of

[18] tps://www.gov.uk/government/publications/biometrics-commissioners-response-to-coronavirus-bill-amendment/commissioners-response-to-coronavirus-bill-amendment

[19] https://www.gov.uk/government/news/biometrics-commissioner-statement-on-the-coronavirus-act-and-the-protection-of-freedoms-act

the NSD is not informed of the retention, which removes any opportunity for that person to redress any grievance by challenging the determination. Because of this unusual aspect of the making of NSDs, PoFA requires that the Biometrics Commissioner must examine each NSD made and if it does not meet the necessary legal requirements, to order the deletion of those biometrics. Section 24 of the Coronavirus Act 2020 removes, in the short run, the requirement to make an NSD and as a corollary removes my oversight of each individual case. The regulations issued under section 24 of the Coronavirus Act only apply to fingerprints and DNA profiles that could be considered under PoFA for the granting of an NSD. PoFA does not cover other biometrics held by the police, in particular the facial images database currently held on the Police National Database. - - -

The effect of section 24, therefore, was to retain biometric information that may be of national security value but at the cost of keeping some biometrics which may prove to be neither necessary nor proportionate to retain. National security was given emergency and temporary priority over individual rights when Parliament passed section 24 of the Coronavirus Act. This was not the intention of the Protection of Freedoms Act 2012 and for that reason the Coronavirus Act, as it effected police retention of biometric material, must be regarded as an emergency and temporary measure justified by Parliament in the face of a new pandemic whose effects were largely unknown at the time. For that reason, I assume Parliament kept to itself the power to extend section 24 but then only for a further six months."

54. It will be for my successor, as Biometrics Commissioner, to provide the Home Secretary and Parliament with information as to the use to which Section 24 has been put during this second six month period and to oversee the process by which Section 24 ceases to be available and is replaced by the normal NSD process as intended by Parliament when it passed the Protection of Freedoms Act in 2012.

INTERNATIONAL EXCHANGES OF BIOMETRICS

55. My Annual Reports have discussed the various kinds of international police exchanges involving biometric material and the recent work by the UK to join the Prüm exchanges of the EU, involving DNA profiles, fingerprints and vehicle registration data. This later work has been pushing forward and a large number of possible DNA matches have been identified and fingerprint exchanges have recently started.

56. However, these exchanges and most other exchanges involving both biometrics and intelligence are EU mechanisms and UK policing's future access will depend on the outcome of the Brexit negotiations, which at the time of writing are still ongoing. The police have publicly expressed their concern if the UK were to lose access to these exchanges[20] and also the European Arrest Warrant, as has the NCA.[21] Against such a contingency the police have been exploring how far EU exchanges could be replaced by bilateral arrangements with individual European countries, but these would be second best as well as resource intensive. Even if some future access to EU exchange mechanisms is negotiated as part of a Brexit agreement, the UK is unlikely to be a party to the planning of the future developments of EU exchange mechanisms and common databases. However, we must wait and see, if there is a Brexit agreement, exactly what its terms are as regards European security and intelligence exchanges.

57. Outside of these EU exchange mechanisms the alternative is those provided by Interpol, but this will be very much slower and less useful than the current EU mechanisms.

58. Once the post-Brexit situation is clearer, the overall structure for international exchanges of biometric material needs re-examining. At present such exchanges are managed by three different policing bodies, ACRO, NCA and the MPS. The rules for exchanging DNA is governed by ministerial policy: that biographic details relating to a sample can only be exchanged if a match is found. Prüm DNA exchanges had more limiting rules, decided by Parliament, but these have since been relaxed by ministers. Fingerprint exchanges are not governed by ministerial policy

[20] See:https://committees.parliament.uk/publications/3466/documents/33316/default/

[21] See:https://committees.parliament.uk/publications/3465/documents/33308/default/

and in practice handled differently from DNA exchanges. This rather over-complex landscape would benefit from streamlining and having a clear ministerial policy on how exchanges of biometrics should be carried out. I have made clear to FINDS-SB that my view is that exchange policy is for ministers and ultimately Parliament.

59. As important as the means and rules for exchanging biometrics, is that UK policing has under-used the mechanisms available. Opportunities for identifying non-UK citizens who have offended in the UK, or UK citizens who have offended in the EU, have therefore been missed that might have protected the public from crime.

THE USE OF 'COMMISSIONERS' IN GOVERNMENT

60. The role of the Biometrics Commissioner was created by PoFA in order to give an independent element to the oversight of the police use of biometrics and particularly to provide a judicial element for some powers provided within PoFA, the exercise of which required pubic reassurance.

61. Such 'commissioner' roles are increasingly common across government and often are created either to respond to parliamentary concerns about aspects of new legislation, or, because it is believed that public reassurance is needed. In addition, such roles can have a judicial element and take some accountability away from ministers. 'Commissioners' are often required to provide advice or reports to ministers and Parliament. This sometimes leaves a problem once the role has delivered on the initial political need, since ministers can come to resent the constraint on their authority or implied criticism of their decision making. It is not uncommon for ministers to seek to abolish or curtail such roles, especially after a change of administration. Furthermore, although such roles are increasing there is no general pattern or even title that they follow. For example, whilst the roles usually have the appearance of independence, the extent to which that is constrained or limited varies from the outset.[22]

[22] Looking across such roles would be an interesting study for the Institute of Government to carry out. It is noteworthy that the new Scottish Biometrics Commissioner will report direct to the Scottish Parliament and indeed be appointed by Parliament in order reinforce their independence,

62. During my period as Biometrics Commissioner, most of my interactions have been with the police who have always been responsive and willing to consider the comments that I have made even when they were critical and notwithstanding that I have no regulatory powers. It says much for the professionalism of British policing that this has been the case. I also have valued the work of the various civil liberty and research groups. Worrying about the protection of liberties or trying to support public debate on such issues by providing evidence is rather rare in England and Wales[23] but necessary in a healthy democracy. Without *Liberty* and *Big Brother Watch* the police use of AFR would not have been tested in the courts and the *Ada Lovelace Institute's* research on the public's attitudes and beliefs about the use of biometrics will help better inform future debates.

63. My relations with ministers, a small minority of officials and Parliament have, however, followed the common pattern for such a role after 7 years. During my tenure I have had very limited or no contact with ministers nor discussion with them of my reports. Response from parliamentarians has been similarly very limited apart from one appearance before the Science & Technology Committee. Of course, my period of office has coincided with two major national issues, Brexit and then Covid-19, which have dominated political discussions almost to the exclusion of everything else. However, a common justification for commissioner-type roles is that they will ensure that both the executive and parliamentary sides of government will continue to pay attention to what might be less immediate or central political issues. Both ministers and parliamentarians may, of course, have felt that the oversight of the police use of biometrics was adequate and not in need of further attention but that hardly reflects the public's expressed concern about both new biometrics and other AI-driven algorithms.

---

a devise reserved in the UK for bodies that arbitrate major issues between political parties, such as the two boundary commissions.

[23] The situation has been different in Scotland with a very active research and consultation process leading up to the legislation for a Scottish Biometrics Commissioner and Northern Ireland has a statutory Human Rights Commission.

64. The promised new biometric legislation[24] may choose not to have a commissioner but if the role does continue then thought ought to be given to how the Commissioner's reports are taken note of and responded to. Furthermore, the Commissioner's oversight role is one thing but the judicial aspects of the role quite another and will be needed as long as legislation allows for the retention of biometrics in a way that the subject is neither aware nor can challenge (NSDs) or where the subject is in such an unequal position relative to the desire of the police to retain their biometrics (section 63G).

65. For the moment we are the only country, as far as I am aware, that has appointed a Biometrics Commissioner and I have had a great deal of contact with a wide range of other countries who are considering their use and governance of biometrics.[25] One aspect that others have commented on is that the UK Biometrics Commissioner it is one of the few examples where both the implementation and subsequent pressures on a piece of legislation has been monitored and commented on over an extended period.[26] We don't have such detailed commentary about the contrast between the law-in-books and the law-in-action in many areas. I hope that those who are involved in what I am sure will be legislation to replace PoFA, can learn from this not so much in terms of content but how to frame legislation to be more effective and efficient. And those lessons have more general applicability across government.

66. More important than these points about political process, the technologies which I have been engaged with have developed and mutated rapidly in terms of their power and application during my time in office. These are some of the primary technologies that will drive both our hoped for economic recovery and the future nature of our social world. In that sense they are strategic. I sometimes worry that the government sees regulation of the use of technology as antithetical to encouraging technical innovation. I think that this is mistaken and our strategic advantage as a nation depends on bringing those two things into

[24] A manifesto commitment made by the present government.

[25] The Scottish Biometrics Commissioner is yet to be appointed and the legislation in Northern Ireland that allows for a biometrics commissioner has still not been implemented.

[26] Treasury-driven impact reviews are very much more limited and formulaic.

alignment. There is no automatic technical imperative at work but rather an ongoing series of development and deployment decisions for personal or institutional advantage and political decisions about how new technologies should shape our future.

THE OFFICE OF THE BIOMETRICS COMMISSIONER

67. My term as Biometrics Commissioner was planned to end on 15th June 2020 but, in the event, I was asked to stay on for a further 6 months. That meant that I expected to be long gone to tend my garden before many of the events described in this interim report occurred. As it happened most of the staff of the Office of the Biometrics Commissioner (OBC) planned to leave around the same time as I had, and because permanent replacements would take some time, temporary arrangements had to be made.

68. I am very grateful to Sir Brian Leveson, who agreed to temporarily loan two of his staff from IPCO: Danny Regan and Kevin Geddes. Danny and Kevin did a superb job both supporting me as Commissioner but also in holding together the Office of the Biometrics Commissioner through a difficult and inevitably stressful time. I know that my remaining permanent colleagues, Tahmida Hussain and Jalal Ahmed, were grateful for their support and also enjoyed working with them. I cannot thank them enough for creating stability to allow the recruitment of new colleagues so that the new Commissioner has a functioning Office.

69. The recruitment process has now been completed and I am pleased to welcome Rebecca Madgwick, the new Head of Office, and Jess Renwick and Valerie Jordan. The main tasks of the new team have been to ensure that my statutory judicial functions were continued and to develop their understanding of the role of the Commissioner in order to welcome and support the new Commissioner. They are an impressive new team who have learned quickly and will be an asset to the new Commissioner.

70. I thank both the present and past staff of the OBC who have supported me during my time as Commissioner. They have been an impressive and dedicated team who have supported me with professionalism and

efficiency. They have been a credit to the quality and commitment to public service of the civil service.

71. Their support will be crucial for the new Commissioner because she/he will need to sort out how they will fulfil the roles of both the Biometrics Commissioner and that of the of the Surveillance Camera Commissioner. Effectively the two commissionerships have been merged and denial by some officials that instead the same person has been appointed to two separate roles is just casuistry. Simplifying accountability is hardly objectionable but it was Parliament that decided that PoFA should create two separate commissioners.
72. Finally, I owe a debt of gratitude to Justin Hawkins who has acted as media adviser to both myself and my predecessor. Justin has the contacts with the press and broadcasters that the OBC lacks. He is professional and calm when giving advice and I have valued his support during my time as Commissioner.

73. It only remains for me to thank all of those that I have worked with during my time as Commissioner. Their unfailing courtesy and good humour has made my time both fulfilling, and I hope useful.

Paul Wiles
Commissioner for the Retention and Use of Biometric Material

10 December 2020

Appendix: The Use of the CPIA Exemption

20 December 2017

Dear Chief Constable,

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

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

One notable exception to this rule was introduced by Section 146 of the Anti-social Behaviour Crime and Policing Act 2014 (amending Section 63U(5)of PACE), which states that where a sample *"is or may become disclosable under the Criminal Procedure and Investigations Act 1996, or a code of practice prepared under section 23 of that act or in operation by virtue of an order under section 25 of that Act",* the sample may be retained until it has fulfilled its intended use, or if the evidence may be challenged in court, until the conclusion of judicial proceedings and any subsequent appeal proceedings. Section 146 continues *'A sample that once fell within subsection (5) but no longer does, and so becomes a sample to which section 63R applies, must be destroyed immediately if the time specified for its destruction under that section has already passed."*

It is clearly open to forces to take differing views as to the circumstances in which a DNA sample *"is or may become disclosable"* under the CPIA or any relevant Code of Practice – and it seems equally clear that forces in fact do so. It has come to the Biometrics Commissioner's attention, through visits to forces and discussions with key stakeholders that forces are interpreting and applying the CPIA exception inconsistently.

In the last 18 months, the Commissioner has seen a rapid rise in the number of samples – both PACE arrestee and volunteer/elimination – held under this exception both in force and with Forensic Service Providers. In addition reviews of DNA samples, which have been held with Forensic Service Providers for over 18 months, have shown that the vast majority of B scrape samples retained under the CPIA exception have not been used for further/specialist analysis. It appears therefore that, at least for some police forces in England and Wales, routine and/or 'blanket' retention of large numbers of DNA samples under CPIA has become 2 the norm. As such very real questions have arisen as to whether Parliamentary intention that DNA samples be routinely destroyed is being circumvented. Consequently it could be argued that the lawfulness of the continued retention of many of the DNA samples at issue has been called into question.

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

Key Principles

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

2. ***Centralised records should be kept of all samples retained under CPIA, both in force and with Forensic Service Providers.*** The Commissioner views that it would be good practice if forces kept such records and he will ask for such information during future visits. The Commissioner suggests that the following information should be recorded:

- Barcode reference
- Location of retained sample
- Sample date
- Date of retention request
- Person authorising retention
- Review dates
- Reason/justification for retention
- Date of request for destruction

The Commissioner suggests that all methods of recording should be fully auditable against the above categories. 3

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

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

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

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

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

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

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

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

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

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

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

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

Yours sincerely,

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