Biometrics Strategy

Better public services
Maintaining public trust

June 2018

OGL

Contents

Ministerial foreword

The use of biometric data is fundamental to the proper functioning of our immigration system, to law enforcement and to those responsible for preventing terrorism. Biometrics allow us to fix a person's identity by linking them to biographical information, to verify who a person is or to identify them amongst many others. As the technology develops this creates opportunities to not only improve safety and security, but to also deliver new and modern services.

Rapid advances in the availability and reliability of biometric technologies bring with them a number of important choices for government, namely how to maximise the benefit to the public, while avoiding risks and protecting the privacy of the individual. Because of their deeply personal nature, and the ubiquity of some biometrics, their use also raises legitimate questions of civil liberties and can affect how the public engage with the police, immigration and others, and impact on their access to and interaction with key government services. Because of the nature of much of the Home Office's work, this can have significant impacts on people's lives.

The use of a given biometric cannot be taken out of its context – who is using the data, for what purpose and how it is handled – but its significance means that we need clear and transparent arrangements to ensure risks to civil liberties are weighed alongside the benefit they can bring. And because of the rapidly changing nature of technology we need to ensure our frameworks for looking at each new use are flexible enough to respond.

This strategy sets out how the Home Office and its partners currently use biometric data, and how we will approach all future developments. It seeks to establish the overarching framework within which such considerations and decisions will be made. This is one of the main ways in which we will retain public trust that we are using new technology to keep the public safe and deliver modern services as well as addressing concerns over their impact on civil liberties. Through implementing and consulting on the commitments made in this strategy, our aim is to increase public confidence in our use of biometric data.

I would like to express my gratitude to all of those who have contributed to the development of this strategy and look forward to working with you all as we develop our use of biometrics in the future.

Baroness Williams of Trafford

Chapter 1: Introduction

1. Biometrics – the recognition of people based on measurement and analysis of their biological characteristics or behavioural data – is increasingly prevalent in everyday life. It is used extensively by businesses to provide new and more efficient services, from unlocking mobile phones to secure banking.

2. Biometrics have long provided a critical role across the Home Office sector from traditional policing forensics, immigration services to national security. The most commonly used forms of biometric are Deoxyribonucleic acid (DNA), fingerprints and face. In 2017, biometrics helped to facilitate the movement of over 46.2 million people through the ePassport Gates at our borders, supported 2.7 million visa applications and in 2016-17 helped to link over 32,000 known individuals to crimes including over 700 rapes.

3. The Home Office sector uses this biometric data in three distinct ways: to fix a person to a claimed identity ('fixing'), to verify a person is who they say they are ('verification') or to identify a person from a biometric ('identification').

   - **Fixing** involves the enrolment of biometric features from individuals and tying their biometrics to the biographical information they provide.

   - **Verification** seeks to answer the question *"Is this person who they say they are?"* It involves checking a biometric (fingerprint, DNA or face) presented by a user against one already on record and linked to that person's records. It takes the form of a 1-to-1 check, often against an identity document such as a biometric residence card or a passport. Biometrics used for verification can also be used for identification checks.

   - **Identification** seeks to answer the questions *"Who is this person?"* or *"Who generated this biometric?"* This process involves checking a biometric presented against a defined data set, taking the form of a 1-to-many check in order to ascertain who the individual is or to whom the biometric data belongs. Identification can be used in screening, for example determining whether a person is also on a 'watch list', or in an investigation where biometric data collected from a crime scene or investigation, is checked against a pre-existing collection.

4. Some biometrics are a very effective way of linking people to their records at key decision points but biometric data is never used as the sole source of evidence in sensitive decision making. Furthermore, in many cases the results are not absolute and depend on the way in which biometric data is collected, handled and processed. For that reason adherence to standards, especially in identification and where there is an impact on individual liberty, is particularly important.

5. Technological advancements are making new forms of biometric data available, such as voice or gait, and have the potential to make others such as facial images – which have always been used to identify or verify people – more useful in identifying or verifying people. They are also improving the speed, reliability and availability of traditional biometric verification and identification.

6. As such biometrics can be used to support the partial automation of high-volume processes, where the confidence they provide of a match significantly improves services and reduces the need for personal data to be processed or shared with other people. They can also be better used in lower volume cases such as investigations or prosecutions albeit with a high degree of human input to assure the matches they provide.

7. Nevertheless, rapid advances in the reliability and availability of biometric technologies, and the ability to search and match across different biometric data sets have the potential to support integrated services and better outcomes – such as finding or eliminating suspects or delivering more efficient services. They can also raise significant issues of public trust in the organisations that use them. It is therefore appropriate to consider the current and future uses, as well as the frameworks for their use within the Home Office sector.

8. Which biometric technology is most appropriate for a particular use will vary significantly across different services. For example, processing a passport application is very different from crime scene DNA collection. Before they are used a number of factors will need to be taken into account including: who is using the biometric data and what legal and regulatory frameworks apply to them; the necessity and proportionality of its use for the purpose being proposed; the risks to privacy including the protection of personal data; the robustness of the techniques including how the biometric data is collected, handled and processed; and steps taken to mitigate risks to privacy. In all circumstances their use must be lawful and there should be a presumption of transparency.

9. The Home Office's aim is to draw on improvements in biometric technologies to protect the public, provide modern services and to increase public trust in the way in which it operates. This requires investments in technology, controlled innovation and a culture and regulatory framework that embeds privacy safeguards within a transparent decision-making process. These need to be combined with clear and independent oversight and consideration of the ethical issues associated with their use.

10. This document describes the Home Office's current approach to using biometrics and how these future developments will be managed. It looks at some of the opportunities to improve public services from current investments and outlines a revised framework for considering new biometric uses, including the processes we will adopt to ensure future use meets legal, ethical and scientific standards.

11. It does not seek to address all the current or future uses of biometrics. Nor does it seek to address the use of biometrics by other Government Departments, the private sector or international partners. Its recommendations will however apply to how the Home Office works with those partners.

12. In preparing this strategy the Home Office has engaged with and gathered evidence from a wide range of stakeholders including the police, forensic service providers, other Government Departments and agencies, regulators and commissioners. The Home Office will also continue to work with the Devolved Administrations in Scotland, Wales and Northern Ireland to ensure that there is alignment in managing areas of mutual interest and devolved matters.

# Chapter 2: Delivering better public services

The Home Office will

- Deliver biometric services designed to be shared and re-used ensuring privacy is addressed in their design and development

- Make it possible to integrate different Home Office fingerprint services to streamline processes and produce quicker, cheaper and more accurate responses for immigration and policing purposes

- Seize opportunities to use biometrics across the Criminal Justice System to verify identity and identify individuals

- Use facial matching to verify more accurately individuals at Ports of Entry

- Improve the automation of fingerprint enrolment at visa application centres to fix and verify identities of foreign nationals applying for visas to come to the UK

- Enable more efficient review and automatic deletion of custody images by linking them to conviction status, more closely replicating the arrangements for fingerprints and DNA

- Consider the case for sharing and matching of facial images held by the Home Office sector and those of other Government Departments

Detail

13. Home Office biometric services and capabilities have been developed over time to meet individual business purposes. This has led to the development of parallel information technology systems, including one fingerprint system for policing and another for visas and immigration. There is also a wide range of ad-hoc, often manual arrangements for the processing of biometrics across the sector including variations in how police and other organisations, collect and analyse biometric data. This can be inefficient and affect the delivery of services.

14. The Home Office is committed to delivering improved biometric services to protect the public and make these services more efficient. This is being enabled through the Home Office Biometrics Programme (HOB) which is delivering improvements to the services supporting fingerprints, DNA and facial images. It is also, with other programmes, playing an important role in improving processes across the Home Office, law enforcement, and other government organisations.

15. The effect of these changes will be to improve continuity, reduce operational costs, support future changes and increase confidence in the robustness of the techniques being used. Through a more consistent, centralised development, this will help increase confidence that legal standards and ethical implications have been taken into account as new uses are developed. This will include ensuring that services have in-built safeguards so that only necessary and proportionate access to biometric data is allowed, for specific roles and purposes. It will also support a more consistent approach to retention.

16. Furthermore, the implementation of a single biometrics platform will remove duplication and costly or inefficient workarounds in operational delivery. This platform is not a new data set, rather a technical platform through which existing data can be more efficiently dealt with. This will also make it easier to use biometric data more widely across the Home Office, operational bodies such as police forces and the National Crime Agency, other Government Departments and international partners. By bringing these together, HOB will deliver biometric services that will enable greater operational efficiency, flexibility, integration and automation.

Figure 1: Scope of Home Office Biometrics Programme
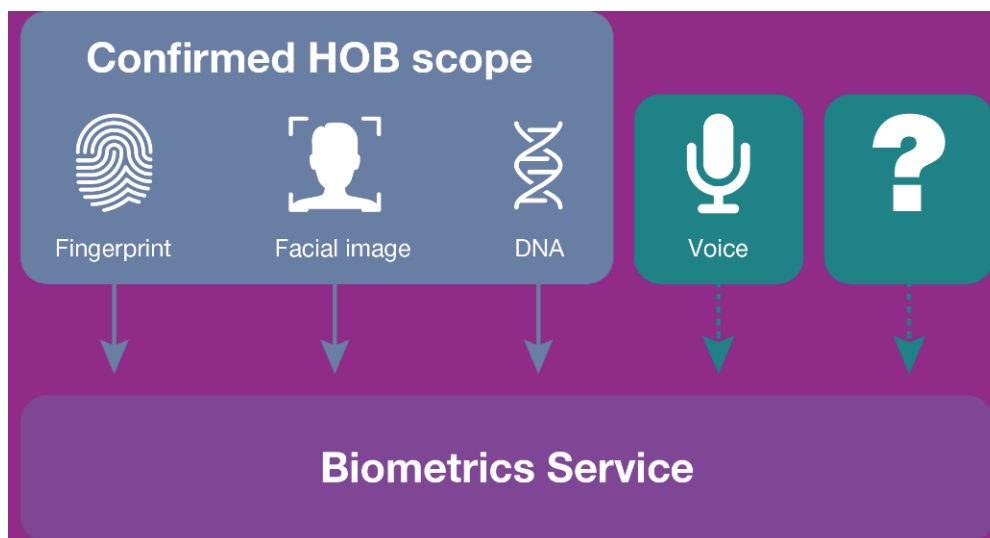
17. Some biometric services (such as DNA and immigration fingerprint services) are already centralised which can help them to operate efficiently by reducing costs and eliminating duplication. Other biometric services are delivered, in part via local offices, or at a regional level. This can help align services with users' needs but the small scale of many functions can increase costs, and restrict overall flexibility. For example, most police fingerprint bureaux cannot support a 24/7 operation. The centrally supported Home Office programmes therefore need to be seen alongside other programmes that improve those local services be they forensics or local IT systems.

Fingerprints

18. Fingerprints are collected in a variety of formats, including flat or rolled impressions taken directly from an individual, or those discovered at a crime scene (known as 'latent marks'). They have long been used to confidently verify identity or to identify individuals in criminal cases, have been used for over two decades in the asylum system, and are used extensively in the private sector and other countries for verification. At present, there are two separate significant fingerprint systems in the Home Office sector. 'IDENT1' is the name given to the system supporting law enforcement, while the Immigration and Asylum Biometrics System (IABS) supports immigration.

19. IDENT1 is used for verification and identification purposes. The system is used by trained practitioners to verify the identity of up to a million people each year taken into custody and arrested or detained. It is also used to identify suspects, witnesses and exclude innocent people through matching latent marks found at

crime scenes or elsewhere by linking such marks to known persons. A discrete dataset is held within IDENT1 for national security purposes.

20. IABS is the Home Office system used for immigration and borders purposes. It supports the fixing of claimed identities of foreign nationals applying to come or to stay in the UK through their fingerprint records. It also contains, where collected, facial images. It is used by Border Force, UK Visas & Immigration (UKVI) and Immigration Enforcement to fix a person to an identity and verify them at the border and in-country.

21. IDENT1 is checked routinely when processing visa or immigration applications. This can identify criminals or those suspected of criminal activity. The police are already able to access immigration records in their custody suite. However, this 'cross-checking' between police and immigration fingerprint databases can be costly and time consuming. Combined with new, cheaper mobile technology, cross-checking is making it possible for law enforcement and immigration officials – whether at the border or as part of immigration enforcement operations – to check against both IDENT1 and IABS systems and HOB has delivered an improved capability to make this cross-checking easier and more efficient.

22. This allows immigration services to check IDENT1 more efficiently as part of the visa application process. For visa applicants, this means an improved customer service and faster processing for lower risk customers. For law enforcement, this reduces the need for people to go to custody to have their fingerprints checked and is helping identify, much more rapidly, suspects, offenders, those who are unlawfully in the UK and even people who have been seriously injured in public places.

Mobile identification by the police

Having detained a person after a short vehicle and foot pursuit, the police, suspecting that the person had provided a false identity, used a mobile fingerprint device to check the identity of the subject against IDENT1. This confirmed that the person had used a false identity and was in fact disqualified. Using existing powers, the police seized his vehicle and, using his correct identity, he was summonsed for driving while disqualified; failing to stop for police; and driving without insurance.

Previously, confirmation that a false identity had been used would have required arresting the person, taking them to a custody suite and conducting enquiries; a process taking up to several hours.

---

23. There are opportunities to extend access to biometric data such as fingerprints, across the Criminal Justice System. For example, the Home Office is working with HM Prison and Probation Service to explore the benefits of biometric mobile identification applications for electronic monitoring and the use of fingerprint scanners in prison receptions. A three-month pilot with the Ministry of Justice to allow real-time checking of fingerprints against local and national databases in a prison for the purpose of verifying identity is due to commence in 2018.

DNA

24. A DNA 'profile' is produced from a sample collected from an individual or at a crime scene, and constitutes 16 pairs of numbers, which correspond to the 16 areas currently involved in the standard DNA profiling process for England and Wales, and a sex marker derived from the sex chromosomes. DNA is used most extensively by policing to link suspects to, or exclude individuals from, crime scenes or evidence collected during an investigation. It is also used to confirm familial relationships in the immigration and nationality systems.

25. In the immigration and nationality system applicants can choose to provide their DNA profile as evidence of familial relationships. Such DNA samples are collected and processed by third companies from an approved list of trusted private providers, with the results sent to caseworkers/examiners to confirm. Such testing is voluntary and usually a last resort, for example when documents are unavailable or inconclusive in linking an applicant to a parent. DNA cannot be required for UK immigration and nationality applications but applicants can volunteer to provide such evidence where it could support their application.

26. The National DNA Database (NDNAD) is a national system which supports identification by allowing the checking of DNA found at scenes of crime with DNA obtained from arrestees. The system also holds, within separate data collections, DNA profiles of vulnerable persons who fear they may be at risk of harm, and a contamination elimination database for police officers and police and forensics staff.

DNA checks

In October 2014 an individual was arrested for a recordable offence and had a DNA sample taken by the police for the first time. The police produced a DNA profile and loaded it onto the National DNA Database. The profile matched against 50 existing crime scene stains. The police were able to put further charges forward against the individual, who then pleaded guilty to charges of rape and burglary with intent to rape.

---

27. The NDNAD is a vital tool in the identification of individuals involved in criminal activity. As at 31 March 2017, the NDNAD held over 6 million subject profile records and 487,000 crime scene profile records. The total number of persons on the system is estimated at almost 5.3 million – some 12.7% of profile records are duplicates of an individual already sampled. In 2016/17, the chance that a crime scene profile, once loaded onto the NDNAD, matched against a subject profile was 66% linking around 32,000 known individuals to crimes in the year to March 2017.

Missing persons

In May 2012 a person went missing while scuba diving off the English coast. A DNA profile was obtained from the person's toothbrush and loaded onto the Missing Persons DNA Database. In July 2014 a wet suit like that worn by the missing person was recovered on the same stretch of coastline containing remains within it. The police obtained a DNA profile and it was found to be a match.

Facial images

28. The face is the primary means used to identify people in many settings. Since the advent of photography, it has been extensively used by police officers and witnesses to identify suspects, or to verify people in immigration and nationality systems. Digital facial images are now used extensively when issuing documents that set out the holders' status, in the verification of identity and in the control of migration, often alongside fingerprints. The police capture facial images under powers set out in the Police and Criminal Evidence Act (PACE) 1984 and these are used in the investigation, detection and prevention of crime and terrorist activities as well as safeguarding.

29. The increased digitisation of facial images combined with algorithms able to reliably match different images is rapidly changing the use of the facial biometric across the Home Office sector. We refer to two forms:

- *Facial Matching* matches a facial image, sometimes referred to as the 'probe' image, against either a single image, such as that held on a passport (1-to-1), or a database of images taken in controlled environments (1-to-many). An example would be the checking of an image of a suspect against images of persons taken on arrest.

- *Automatic Facial Recognition* (AFR) is the checking of facial images, generally obtained in an uncontrolled public environment, against a watch list of people whose images have been taken in controlled or uncontrolled environments.

30. When used for verification, a 1-to-1 match can be made between a secure identity document and the person or between the person and a stored image. The reliability of matching is affected significantly by the quality of the images – both the reference image stored on a database or watch list and the captured image. Generally, there are therefore distinctions drawn between matches of controlled images such as passport photos or custody images and those captured through surveillance cameras or still photos.

31. Within policing, facial images are most often collected in a custody suite following an arrest. These controlled facial images are held on local systems. Many are uploaded to the Police National Database (PND) – a system used to support cross-force cooperation in the detection, investigation and prosecution of crime. As of February 2018, there were 12.5 million images stored on the PND and searchable using facial recognition software. This does not represent the number of people due to duplicates on the system and is only a proportion of the total 21 million images held on the system which includes further duplicates as well as marks, scars and tattoos.

32. Following the Custody Image Review[1], people who have been acquitted or where charges have been dropped may apply for their custody images to be deleted from law enforcement databases. That will trigger a review of the image retention allowing the police to retain the image on their system under certain specified circumstances against a presumption of deletion.

33. At present, it is not possible to automatically prompt the review of images from local law enforcement databases. When the Law Enforcement Data Service, which will replace the Police National Computer (PNC) and the PND, is in place it will enable more efficient review and where appropriate, automatic deletion of

---

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

custody images by linking them to conviction status, more closely replicating the system for DNA and fingerprints.

Police use of facial images

Police responded to reports of an unconscious male in a river, and paramedics attempted to save his life without success. Police took steps to identify him, starting with taking a photo of his face on a mobile device. They succeeded in identifying him by comparing that image with the local police custody images database. This enabled the police to trace the victim's family significantly faster

---

34. In future, HOB will provide a common facial matching service enabling the Home Office to realise efficiencies and ensure a more consistent approach to the testing, access controls and privacy protections associated with it. This will allow improvements in the technology and matching algorithms to enhance processes at Ports of Entry, Visa Application Centres and within passport applications.

35. Looking further ahead, we will consider the use of AFR for verifying identity and identifying known criminals of interest. We will run proof of concept trials to develop this work, including at the UK border and will consider enabling access to facial image collections at custody suites and on police mobile devices to help identify or verify identities for wider law enforcement purposes.

36. Although biometric identification in policing and immigration is predominantly enabled by biographic and fingerprint data, technologies incorporating AFR also have the potential to aid identification. AFR is an emerging technology and police forces have been trialling these systems. For example, South Wales Police have used AFR to compare images of people in crowds attending major public events such as concerts, with pre-determined watch lists of suspected mobile phone thieves. Watch lists, created for time limited and specific purposes, could also include individuals banned from attending an event or known criminals who have previously operated in crowded spaces.

37. The use of AFR technologies is governed by a number of codes of practice including those applying to the police such as PACE. In particular the use of AFR is covered in the twelve principles laid down in the Surveillance Camera Code of Practice[2], to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras[3] applies to their use by the police and other authorities. We recognise that the governance and oversight of these applications and the use of facial images as a biometric by law enforcement could be strengthened further. This is addressed further in Chapter 3.

---

[2] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
[3] https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
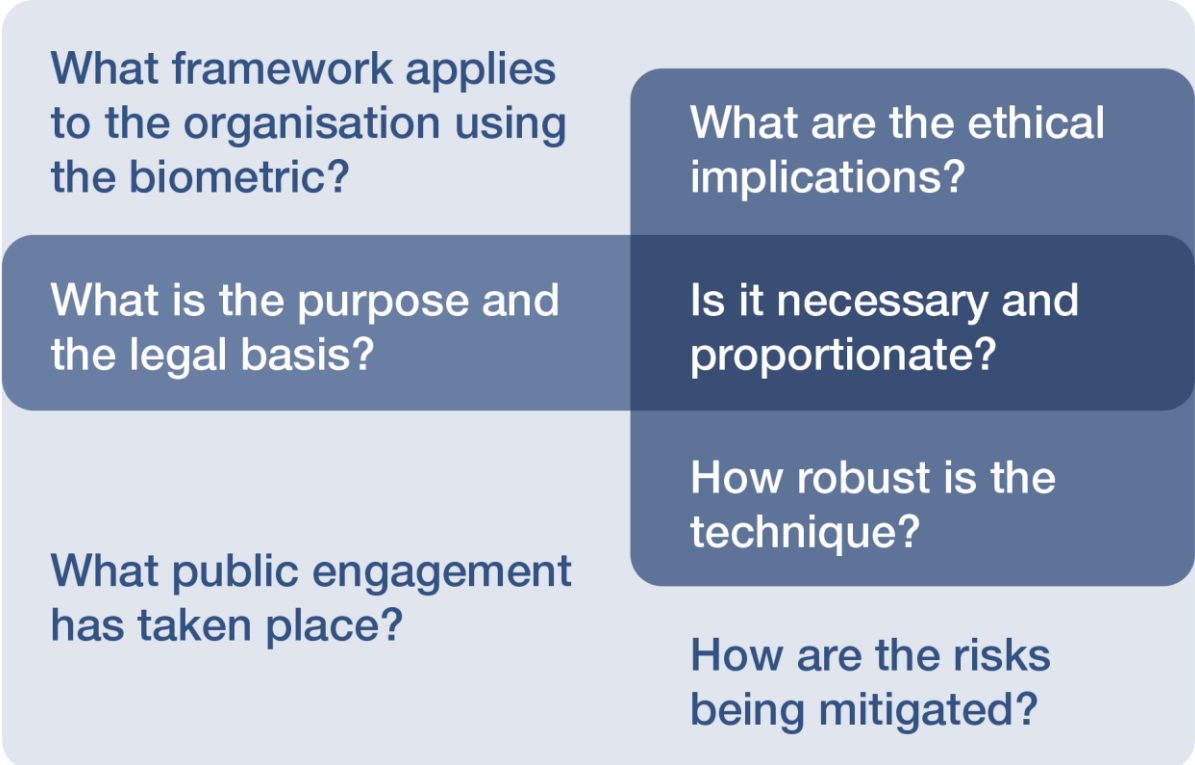
Chapter 3: Maintaining public trust

The Home Office will

- Establish a new oversight and advisory board to coordinate consideration of law enforcement's use of facial images and facial recognition systems. It will be asked to provide policy recommendations regarding the use of facial biometrics and future oversight arrangements

- Undertake Data Protection Impact Assessments (DPIAs) prior to the use of a new biometric technology or a new application of an existing biometric technology, inviting scrutiny from an independent ethics panel, regulators and commissioners

- Undertake DPIAs for each element of the Home Office Biometrics Programme

- Update the Home Secretary's Surveillance Camera Code of Practice in collaboration with the Surveillance Camera Commissioner (SCC)

- Continue to implement the findings of the Custody Image Review and ensure that the SCC and ICO's guidance on the use of images is followed

- Develop options to simplify and extend governance and oversight of biometrics across the Home Office sector through consultation with stakeholders over the next 12 months

Detail

38. The increased use of biometrics can raise significant issues of public trust in the organisations use them. Data protection legislation categorises biometric data as a 'special category' of data because it is more sensitive than some other forms of data, and therefore needs more protection. Given the personally intrusive way in which some biometric data is acquired, the ability to retain them for long periods and the potential significant impacts from their use or misuse, they require special consideration.

39. The Home Office recognises its role in providing the public with the confidence that their personal data including biometric data is adequately protected and handled in accordance with the law. That role includes carrying out impact assessments for the systems we build and run, working with other organisations in the sector to ensure they have given appropriate consideration to the use of biometrics and supporting the development of appropriate standards, assurance and oversight arrangements.

40. Like the technology, legislation, governance and oversight have developed iteratively. We describe principal features of present arrangements for DNA, fingerprints and facial images, including the roles of those who play prominent role in oversight and regulation, below. Much of this works well and our use of biometrics is lawful. However, given the potential to rapidly increase data and technology integration, our view is that this system may not be sufficiently robust or flexible in the foreseeable future. In addition to addressing concerns with the oversight of facial biometric applications, we will develop options to simplify and extend governance and oversight of biometrics through consultation with stakeholders over the next 12 months.

Figure 2: Home Office considerations before introducing a new biometric technology or a new application of an existing biometric technology

What framework applies to the organisation using the biometric?

What are the ethical implications?

What is the purpose and the legal basis?

Is it necessary and proportionate?

How robust is the technique?

What public engagement has taken place?

How are the risks being mitigated?

Governance

41. Governance arrangements vary between biometric modalities, reflecting the maturity of the technologies and with the organisation making use of the biometric data. The most mature arrangements are in the field of DNA and fingerprints in law enforcement. Until recently, the NDNAD was overseen from a legal, operational, policy, ethical and privacy perspective by the National DNA Strategy Board. In 2016, fingerprints were added to its remit and it is now known as the 'FINDS-Strategy Board' (FINDS-SB). FINDS-SB monitors the performance of biometric databases and provides oversight of how the police use their powers under Part V of PACE for the taking, use, retention and destruction of DNA samples and fingerprints. FINDS-SB also issues guidance to the police on the use of the databases in meeting the requirements of legislation.

42. Given the potential for the use of facial biometric technologies in law enforcement we will establish a new oversight and advisory board to coordinate consideration of issues relating to law enforcement's use of facial images and facial recognition systems. Representatives from the police, Home Office, the SCC, the Biometrics Commissioner (BC), the ICO and the Forensic Science Regulator (FSR) will be invited to be part of, or advise the board in its consideration. The SCC and the ICO will be asked to comment on compliance with existing legislation and codes and, with the BC and FSR, will be asked to provide independent advice to the board with regards to legislation and standards. The Biometrics and Forensics Ethics Group (described in further detail below) will also be represented.

43. The oversight and advisory board will be asked to consider issues relating to law enforcement's use of facial images and AFR efficiently and with greater transparency than to date. This will include the policies for the retention, deletion and the use of images, within for example, AFR technologies. The board will be asked to provide government with policy recommendations pertaining to the use of facial biometrics. It will also be invited to consider new biometric modalities at an early stage as they emerge in law enforcement.

44. Within the Home Office, consideration of new biometric technologies will be undertaken by the relevant business area including through the completion of DPIAs and, where appropriate those will be considered by the relevant groups including the recently established Home Office Data Board.

Privacy protection and impact assessments

45. The privacy impact from the use of individuals' biometric information must be considered before, during and after the operation and development of biometric services, whatever their usage. The collection, retention and use of biometric data is legal if the interference with an individual's privacy is necessary, proportionate and in pursuit of a legitimate aim (such as the prevention and detection of crime) and complies with legislation governing the use and retention of biometric data. This framework is summarised in Figure 2 (above).

46. Before the entry into application of the General Data Protection Regulation (GDPR) and the Data Protection Act in May 2018, the ICO recommended that a Privacy Impact Assessment (PIA) be undertaken when personal data was being processed in any new or innovative ways. The Home Office has followed this recommendation. This supports privacy by design, ensures compliance with human rights legislation and reduces the likelihood of breaching data protection principles. The Home Office has undertaken PIAs across each area of the HOB Programme, and will publish a separate PIA considering the overall privacy impact of the Programme.

47. The Data Protection Act now requires the completion of a DPIA where data processing is likely to result in a high risk to the rights and freedoms of individuals. The Home Office will complete a DPIA for each element of the HOB Programme, adding to or amending the existing PIAs. Further the Home Office will produce DPIAs for new biometric technology applications and have a presumption of making relevant aspects available for independent scrutiny.

48. The Home Office will consider the case for adopting additional biometric modalities on a case by case basis where they may have a positive impact on the delivery of our objectives. We will undertake DPIAs prior to the trial of any new biometric technology or a new application of an existing biometric technology and we will expect an ongoing process of evaluation. For law enforcement, the new oversight and advisory board will be the co-ordination point for consideration of new applications. For immigration, the Home Office Data Board will perform this function. Figure 3 below illustrates how this process will work and what considerations will continue to guide decision making.

Figure 3: Home Office process for introducing a new biometric technology or a new application of an existing biometric technology
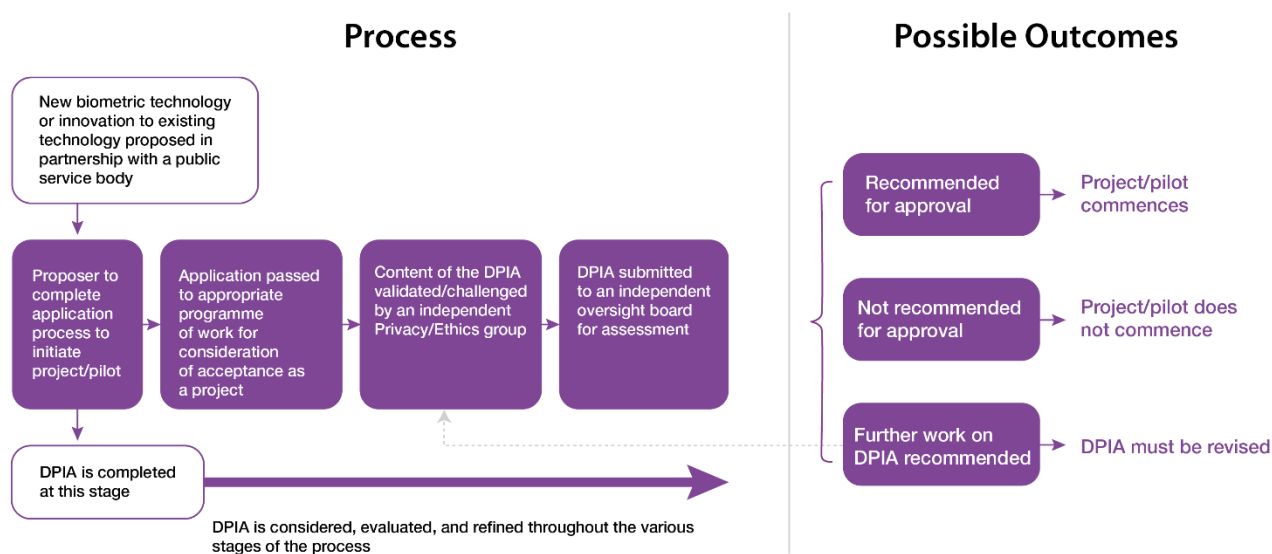
Ethics

49. Whilst the use of biometrics in a range of situations may meet legal criteria and the underpinning techniques are robust, the decision may nevertheless raise ethical questions. We are committed to continue the incorporation of such considerations into new potential uses. This was already the case for DNA which was considered by the National DNA Database Ethics Group.

50. In July 2017, we expanded the National DNA Database Ethics Group and renamed it the Biometrics and Forensics Ethics Group (BFEG) to include the consideration of ethical aspects of the application and operation of technologies which produce biometric and forensic data and identifiers including facial recognition. In April 2018 the BFEG published its Ethical Principles[4] to apply to the use of biometric and forensic procedures. Given the importance of ethical issues the BFEG will be represented on the new facial image oversight and advisory board as they currently are on the FINDS-SB.

Oversight and standards

51. The appropriate use and development of biometric technologies in the Home Office sector relies on a wide range of organisations across the private and public sector. Public trust relies on the professionalism of staff across this end-to-end process. To provide assurance a range of standards, guidance and assurance mechanisms have developed including independent Commissioners and Regulators. The introduction of Data Protection Officers across public authorities and for data controllers will have a positive impact on the use of this sensitive personal data but there will be a need to maintain and develop specific standards for key sectors that use biometrics.

52. The Home Office sector works with a wide range of independent organisations to provide oversight and guidance in relation to biometrics. The four key Commissioners and Regulators who oversee our use of biometrics. These include:

---

[4] https://www.gov.uk/government/publications/ethical-principles-biometrics-and-forensics-ethics-group

- **The Biometrics Commissioner** (BC) is an independent reviewer who is required to produce an annual report on police and national security use of DNA and fingerprints. The Commissioner also reviews National Security Determinations in determining whether and for how long DNA profiles and fingerprints should be retained for national security purposes.

- **The Surveillance Camera Commissioner** (SCC)'s role is to encourage compliance with the Surveillance Camera Code of Practice. The Commissioner has developed self-assessment tools, standards for the CCTV industry and a third party certification scheme.

- **The Forensic Science Regulator** (FSR) ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards. The Regulator produces Codes of Practice, technical guidance, and provides advice and support.

- **The Information Commissioner's Office** (ICO) upholds information rights, enforces data protection regulations and promotes understanding of the risks, rules, safeguards and rights in relation to processing. They issue guidance, advice and can carry out enforcement action.

53. The development of new technologies and the identification of risks can arise across the different areas. For example voice comparison is also already used in forensic science and some standards have been set out by the FSR. We will therefore welcome and wish to support the close co-operation between the different Regulators and Commissioners in the development and maintenance of new guidance and tools to support the appropriate use of biometrics across the sector.

54. We welcome the introduction of the Forensic Science Regulator Bill on 9 March 2018 which seeks to put the FSR on a statutory footing to ensure that forensics across the criminal justice system are subject to an appropriate regime of scientific quality standards. The Bill includes provision for the FSR to investigate any forensic provider who risks prejudicing the course of legal proceedings and require them to provide information and documents to support the investigation. Further, the FSR will be able to issue a compliance notice requiring providers to take certain actions in order to improve their standards, and may as a last resort prohibit them carrying out certain forensic science activities until they do so.

55. In law enforcement, competency levels for fingerprint practitioners and experts are developed and overseen by the NPCC National Fingerprint Board which includes the College of Policing. Immigration Fingerprint Bureau staff also make use of police training. The FSR is also responsible for producing and maintaining Codes of Practice for forensic techniques and has produced standards to support the application of fingerprint comparison supported by ISO standard 17025 where applicable. In addition, by relying on the international standard ISO17025 and the FSR's Codes of Practice, the United Kingdom Accreditation Service (UKAS), ascertains that the organisation has competent staff.

56. DNA recovery, analysis and interpretation in law enforcement is subject to standards and codes of practice set by UKAS, the FSR and the Forensic Information Databases Services Unit. DNA profiles are loaded onto the NDNAD which searches the DNA profile records from crime scenes against the DNA profile records from individuals or other crime scenes. A match occurs when the 16 pairs of numbers (and sex marker) representing an individual's DNA are an exact match to those in the DNA left at the crime scene or when a crime scene profile matches another crime scene profile. The profile is almost unique with the chance of two unrelated people having identical profile records being less than one in a billion. The scientific and technical confidence levels provided by DNA matching is therefore very high. Sometimes it is not possible to recover a complete DNA profile from the crime scene but partial matches provide valuable leads for the police.

57. Matching of facial images is less mature and the standards and procedures are more varied. HMPO adheres to the International Civil Aviation Organisation (ICAO) standards that ensure facial recognition images captured from each passport will be acceptable at UK and international border controls for both manual and automatic checking purposes. Within law enforcement the FSR's Codes of Practice and Conduct provide a set of validation requirements in relation to image comparison. Although PACE Code D provides guidance on the identification of suspects, policing in England and Wales do not have common standards for the capture, storage or exchange of facial image data.

PACE 1984

The Police and Criminal Evidence Act (PACE) 1984 lays down police powers to take and use biometric data. It allows for DNA and fingerprints to be taken from people arrested for a recordable offence, and for DNA profiles and fingerprints to be retained while the person is under investigation. PACE provides safeguards, notably that the data can be used only for purposes related to crime, national security and the identification of the person to whom they relate.

---

58. As the use of facial matching and AFR increases in maturity, the Home Office is committed to ensuring that the law and standards keep pace. Given the importance of Surveillance Camera Systems in the capture of facial images notably for investigations, the Home Office will, in collaboration with the SCC, update the Surveillance Camera Code of Practice. We will also work with the FSR and others to ensure that standards are in place to regulate the use of AFR in identification before it is widely adopted for mainstream law enforcement purposes.

Glossary

AFR	Automatic Facial Recognition. This is the checking of facial images, generally obtained in an uncontrolled public environment, against a watch list of people whose images have themselves been taken in controlled or uncontrolled environments
APP	College of Policing's Authorised Professional Practice
BC	Biometrics Commissioner
BFEG	Biometrics & Forensics Ethics Group. This is a statutory non-departmental public body providing ethical guidance to the use and retention on biometric modalities.
Biometrics	The recognition of people based on measurement and analysis of their biological characteristics or behavioural data.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images, fingerprints or DNA, amongst other types
Biometric technology	Technology that enables the capture of biometric data from an individual
CCTV	Closed circuit television
DNA	Deoxyribonucleic Acid
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DVLA	Driver and Vehicle Licensing Agency
EU	European Union
Facial matching	Facial matching is the technique used to match a particular facial image against a database of images taken in controlled environments
FINDS-SB	Forensic Information Databases Strategy Board
FSR	Forensic Science Regulator
GDPR	General Data Protection Regulation 2016
HMPO	Her Majesty's Passport Office
HOB	Home Office Biometrics Programme
Home Office sector	The Home Office sector comprises three systems: Public Safety, Homeland Security and Borders, Immigration and Citizenship

IABS	Immigration and Asylum Biometric System. The UK's fingerprint system supporting immigration
ICO	Information Commissioner's Office
IDENT1	IDENT1 is the name given to the UK's fingerprint system supporting law enforcement
Livescan	Livescan is a technology enables officers to carry out real time checking of fingerprints against local and national databases of prints already on file
NDNAD	National DNA Database
PACE	Police and Criminal Evidence Act 1984
PIA	Privacy Impact Assessment
PNC	Police National Computer
PND	Police National Database
POFA	Protection of Freedoms Act
Recordable offence	An offence for which the police are required to keep a record on the PNC. The vast majority of offences fall in this category, as the number of offences for which the police are not required to keep a record is very limited
SCC	Surveillance Camera Commissioner
Surveillance Camera System	This is a system of cameras used for the purpose of observing an area. Signals are not publicly distributed but are monitored, primarily for surveillance and security purposes
UKAS	The United Kingdom Accreditation Service. The national accreditation body responsible for assessing agreed standards, technical competence and integrity of organisations that provide certification, testing, inspection and calibration services

Annex

Overview of current Home Office sector biometric uses, legislation, oversight and governance

Biometric Modality	Home Office Function	Use	Legislation and data retention	Oversight	Governance
FINGERPRINTS	**Law enforcement**	The **police** take fingerprints of arrested persons and fingerprints found at crime scenes for investigatory purposes. The police also take fingerprints of arrested persons to confirm identity.	Retention periods depend on the nature of convictions under PACE and POFA • Police and Criminal Evidence Act (PACE) 1984 • Protection of Freedoms Act (POFA) 2012 • Data Protection Act 2018	Biometrics Commissioner Forensic Science Regulator The Information Commissioner's Office	Forensic Information Database Service Strategy Board Biometrics and Forensics Ethics Group

	Immigration	**UK Visas and Immigration (UKVI)** takes fingerprints from visa applicants. **UKVI** also take and store the fingerprints and images of long term visitors and migrants to the UK, in order to issue them with a Biometric Residence Permit. At UK ports of entry, **Border Force** check that the fingerprints captured from those travelling on visas or entry clearances match the fingerprints submitted on visa applications.	Fingerprints are normally retained for up to ten years except for fingerprints taken under the Immigration and Asylum Act 1999 • Criminal Justice and Immigration Act 2008 • Nationality, Immigration and Asylum Act 2002 • Borders Act 2007 • Immigration and Asylum Act 1999 • Immigration Act 2014 • Data Protection Act 2018	Independent Chief Inspector of Borders and Immigration The Information Commissioner's Office	Home Office Data Board Biometrics and Forensics Ethics Group
	National Security	As per law enforcement	A national security determination has effect for a maximum of 2 years beginning with the date on which it is made and can be renewed • Police and Criminal Evidence Act 1984 • Protection of Freedoms Act 2012 • Proposed Counter Terrorism and Border Security Bill 2017-2019	Biometrics Commissioner The Information Commissioner's Office	

Biometric Modality	Home Office Function	Use	Legislation and data retention	Oversight	Governance
DNA	Law enforcement	The **police** take DNA samples from detainees in custody and from crime scenes. DNA profiles cannot be linked to an individual once the record has been deleted. If the profile information meets the defined quality threshold it is loaded and searched against national DNA collections.	Retention provisions are governed by: • Police and Criminal Evidence Act 1984 • Protection of Freedoms Act 2012 • Data Protection Act 2018	Biometrics Commissioner Forensic Science Regulator The Information Commissioner's Office	Forensic Information Database Service Strategy Board Biometrics and Forensics Ethics Group
	Passports and immigration	**HMPO:** DNA testing is voluntary and usually a last resort when documents are unavailable or inconclusive in linking an applicant to a parent, for example to confirm parentage for nationality purposes. **UKVI:** On rare occasions DNA is accepted in immigration and asylum applications.	Retention - DNA profiles are not held by HMPO after the passport is issued • Data Protection Act 2018 • Dublin III Regulation	Independent Chief Inspector of Borders and Immigration The Information Commissioner's Office	Home Office Data Board Biometrics and Forensics Ethics Group

	National Security	A separate, discrete database is maintained for DNA profiles and crime scene stain records for national security and counter-terrorism purposes.	A national security determination has effect for a maximum of 2 years beginning with the date on which it is made and can be renewed • Police and Criminal Evidence Act 1984 • Protection of Freedoms Act 2012 • Data Protection Act 2018 • Proposed Counter Terrorism and Border Security Bill 2017-2019	Biometrics Commissioner The Information Commissioner's Office

Biometric Modality	Home Office Function	Use	Legislation and data retention	Oversight	Governance
FACIAL IMAGES	**Law enforcement**	The **police** take custody images locally. They are uploaded onto the PND and made available to other forces. Law enforcement may also compare potential suspects against images from CCTV or mobile phone footage for evidential and investigatory purposes. Automatic Facial Recognition (AFR) has been trialled by some forces at major public events to identify known criminals against pre-determined watch lists.	Facial images retained by the police are governed by the Code of Practice on the Management of Police Information (MOPI) and guidance set out in the College of Policing's Authorised Professional Practice (APP). People who are not convicted can apply for deletion of their image and that this should normally be agreed, unless there is an exceptional reason to retain the image for a policing purpose. Retention of convicted persons' images is reviewed at specified intervals, which depend on the seriousness of the offence. • Police and Criminal Evidence Act 1984 • Protection of Freedoms Act 2012 • Data Protection Act 2018	The Information Commissioner's Office Surveillance Camera Commissioner's Codes of Practice	Biometrics and Forensics Ethics Group (BFEG) **The new oversight and advisory board will consider law enforcement use of facial images, facial recognition systems and use of new biometric modalities as they emerge.**

	Passports and immigration	UK Visas and Immigration (UKVI) takes and store images to issue Biometric Residence Permits. Images taken for nationality purposes are then passed on to HMPO for any subsequent passport application. Border Force compares the images of travellers using the 'ePassport Gates' to their passport photographs to help expedite passport controls. HM Passport Office (HMPO) stores the facial images of passport holders and uses them to help verify identity on every passport renewal application as well as to check against fraudulent or suspected fraudulent applications.	Photographs taken for the purposes of immigration are retained for as long as the Home Secretary considers it necessary for use in connection with an immigration or nationality function or until the person becomes a British Citizen and obtains a British passport. HMPO retain facial images from adult passport applications indefinitely • The Immigration (Biometric Registration) (Amendment) Regulations 2015 • The Royal Prerogative • Data Protection Act 2018	Independent Chief Inspector of Borders and Immigration The Information Commissioner's Office	Biometrics and Forensics Ethics Group (BFEG) Home Office Data Board

| | **National Security** | As per law enforcement | A national security determination has effect for a maximum of 2 years beginning with the date on which it is made and can be renewed

• Police and Criminal Evidence Act 1984
• Protection of Freedoms Act 2012
• Data Protection Act 2018 | Biometrics Commissioner
The Information Commissioner's Office |