Annex B: Privacy Impact Assessment Screening Questionnaire (published separately)

Home Office Biometrics Programme

Privacy Impact Assessment Screening Questions

This PIA document was last updated on 15th August 2017

Privacy Impact Assessment Screening Questions

Purpose

1. Information Commissioner's Office (ICO) and Cabinet Office recommend, as best practice, the consideration of privacy issues when working on a project, programme or policy development or any measure that involves the use and processing of data. This document provides an introduction to the Home Office Biometrics (HOB) Programme in response to the screening questions set out in the Home Office Privacy Impact Assessment (PIA) guidance.

2. To strengthen public trust by showing that data processing by the Home Office Biometrics Services, including the provision of data to law enforcement or other government partners, is legal, ethical and robust.

Summary

3. Biometrics: is the recognition of individuals based on analysis of their biological characteristics and includes fingerprints, DNA and facial images, amongst other types. Biometrics can be used in various ways to recognise individuals, repeatedly, to a high degree of confidence. It is therefore one of the best ways of verifying previously confirmed identities, by associating an individual's biometric and biographical details together. Biometrics is used extensively across Government for the purposes of crime prevention and investigation, protection of the Border, counter terrorism and protection of UK overseas interests and the delivery of public services – for example HMRC are using fingerprints and Voice ID to confirm identity when accessing their tax credits and self assessment services.[1]

4. The Home Office has existing biometrics systems whose contracts come to an end in 2019. The HOB Programme aims to evolve these systems to provide continuity beyond 2019 and enhance their capability through a number of phases. The systems being replaced hold biometric information which is sensitive personal

[1] https://www.gov.uk/government/news/voice-id-showcases-latest-digital-development-for-hmrc-customers

data about individuals, *all* of which could be privacy intrusive, and *some* of which the individual can be compelled to supply.

5. The HOB programme will provide a common Home Office capability which will facilitate greater efficiency in the way that biometric services are delivered to authorised users in the wider public sector. So while this is a Home Office led biometrics convergence programme, it will benefit the wider government and other public sector customers.

6. Notwithstanding

a) that new biometric modalities will not be collected;

b) that biometrics are used in a way which is compliant with relevant legislation; and

c) that any changes regarding permission to access and use the information are not within the scope of the HOB programme.

The nature of the sensitive personal information means that a PIA is necessary for the programme. The need is set out in more detail in the answers to the screening questions.

Introduction

7. The HOB Programme is delivering the services supporting fingerprints, facial images and DNA (the main biometric modalities currently, and extensively, used in the UK public sector), developing their capabilities across the Home Office and law enforcement

8. These capabilities are currently provided through IDENT1, the National DNA Database (NDNAD) and the Immigration and Asylum Biometric System (IABS - which also supports Her Majesty's Passport Office (HMPO) via the HMPO Facial Matching system). These services enable the Home Office and law enforcement to capture, authenticate, verify, search and match individual biometrics for the purposes of solving crime, protecting borders and preventing terrorism.

9. HOB is focusing on the delivery of *services* and *capabilities*, which are designed to be *shared and re-used* across the Home Office and law enforcement. This approach should allow for appropriate access that is necessary and proportionate for specific

roles and purposes (such as in relation to national security, serious and organised crime investigation, volume crime and immigration).

10. The priority for the HOB Programme, ahead of delivering new benefits through the creation of new services, will be to provide continuity of vital services and to rationalise the existing biometrics technology estate in order to reduce running costs.

11. The objectives of the HOB Programme support all of the Home Office Departmental goals to:

- Cut crime and the harm it causes, including cyber-crime and serious and organised crime
- Manage civil emergencies within the remit of the Home Office
- Protect vulnerable people and communities
- Reduce terrorism
- Control migration
- Provide world-class public services and contribute to prosperity
- Maximise the benefits of the United Kingdom leaving the European Union

---

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

PIA screening questions

Will the project involve the collection of new information about individuals?

No

Current Situation

1.1 The information currently collected about individuals, by the systems within the scope of HOB, is as follows:

DNA[2]

England & Wales

1.2 The National DNA Database™ (NDNAD), stores a collection of DNA subjects of people and crime scene stain records. The NDNAD is administrated by the Forensic Information Databases Service (FINDS) - formerly known as the National DNA Database Delivery Unit (NDU) in the Home Office. Oversight of the NDNAD is through the Forensic Information Databases (FIND) Strategy Board which is a body created by the Secretary of State for the Home Department in compliance with the provisions of s.63AB of the Police and Criminal Evidence Act 1984 ('PACE').

1.3 DNA samples collected at the scene of a crime are sent to a Forensic Service Provider (FSP) for DNA profiling. The generated profile is sent to the FINDS-DNA Unit for NDNAD storage and matching purposes. All sampling and profiling of DNA is subject to ISO17025[3] and is further subject to technical requirements set by the FIND Strategy Board and Forensic Science Regulator.

1.4 Usually, DNA samples are collected from people who are arrested for a recordable offence within custody suites in police stations, normally using a mouth swab. A hair sample will be taken on a rare occasion should the person not cooperate in giving a mouth swab[4]. Two samples are taken for each person. The sample is sent to a FSP provider for DNA profiling. The generated DNA profile (in the form of numerical values rather than the raw DNA processing results) is then sent to the FINDS-DNA Unit for NDNAD for storage and matching purposes.

---

[2] Source Forensic Science Regulation Unit & FINDS

[3] ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories is the main ISO standard used by testing and calibration laboratories. In most major countries, ISO/IEC 17025 is the standard for which most labs must hold accreditation in order to be deemed technically competent

[4] **Non-Intimate Samples**
A non-intimate sample is hair (that is not pubic hair); a sample taken from the nail or under nail; a swab taken from any part of the body, including a mouth swab, but not from any other body orifice; saliva and a footprint.
Intimate Samples
An intimate sample is defined as: blood, semen, any other tissue or fluid, urine, pubic hair, dental impression or swab taken from any orifice other than the mouth.

1.5 The collection of mouth swabs and hair samples is done under provisions set out in ss.62/63 of PACE. The DNA profiling is subject to ISO17025, augmented by technical requirements (as above in 1.3).

1.6 The Forensic Science Regulator publishes Codes of Practice and Conduct which covers all FSPs, including police scientific functions (i.e. currently not custody). This incorporates established good practice as well as requirements set by the Home Office, FIND Strategy Board, EU decisions, the Lord Chief Justice and case law.

1.7 A DNA profile consists of a string of 16 pairs of numbers (though this may increase in the future) and 2 letters (XX for women, XY for men) to indicate gender which can be used to distinguish an individual (unless an identical twin). It is this information which is stored on the NDNAD[5].

1.8 The sample itself is kept for a maximum of 6 months unless it is required for evidence in court[6], in which case it may be retained for the duration of the proceedings.

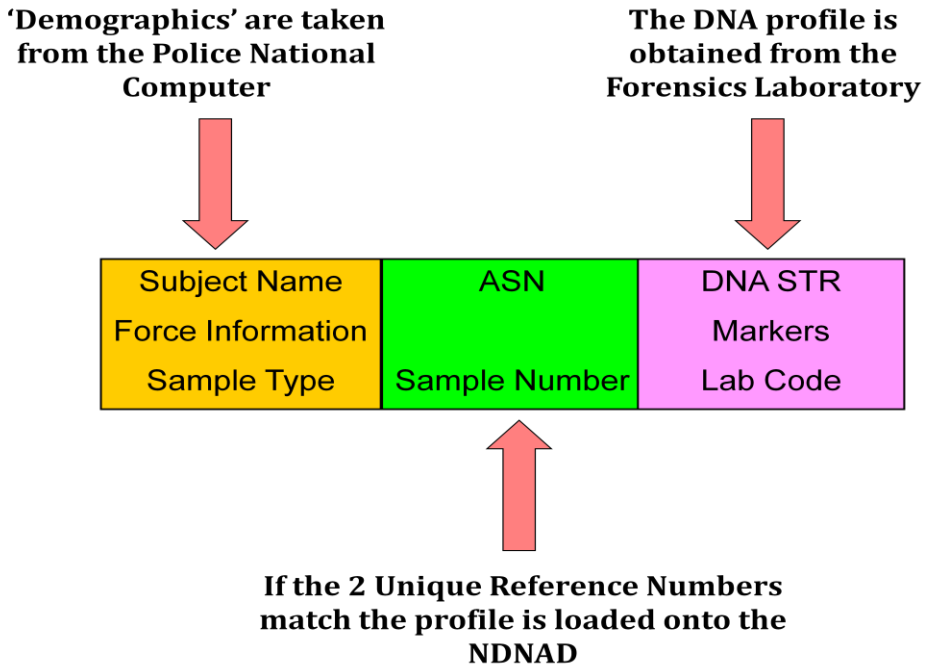
1.9 Retention: The Protection of Freedoms Act 2012 (POFA), which amended PACE, established a new regime to govern the retention and use of DNA samples and DNA profiles (and fingerprints – see below) taken by the police in England & Wales. These provisions are retained as summarised in Annex i.

Loading DNA profiles

1.10 There is an integrity check for loading DNA profiles which includes the matching of the Arrest Summon Number (ASN) and a unique sampling reference together with the DNA profile result.

[5] The current DNA profiling method used for the Scottish DNA Database –known as DNA24 -analyses 23 areas of a person's DNA and the gender marker

[6] The sample may have to be retained if such retention is required under the Code of Practice issued under s. 23 Criminal Procedure and Investigations Act 1996 and is specified within POFA 2012 that updated PACE.



Information held on the NDNAD

1.11 NDNAD contains a unique identifier (barcode) associated with a DNA profile. The barcode is used with the ASN to confirm that the same record is being stored on NDNAD from the PNC element and the information being submitted from the DNA laboratory. PNC is deemed the master of data for those records relating to arrestees taken from Forces within England and Wales:

- the Arrest Summons Number (which provides a link to the record on the Police National Computer (PNC))
- the person's name
- their date of birth
- their ethnic appearance
- their sex
- information about the police force that collected the sample
- information about the laboratory that analysed the sample and the associated batching details
- the sample type (blood, semen, saliva etc.)

- the test type
- the DNA profile

Scotland

1.12 Policing in Scotland is a matter for the Scottish Government. Scotland has a separate database managed by the Scottish Police Authority (SPA) which is independent to the NDNAD but cross-share forensic DNA information with them. The DNA profile records from Scotland, relating to all of their records relating to people and those of crime stain records where there has not been a positive match within the Scottish Database, are submitted to the NDNAD for storing and matching. Retention of the records has to comply with the legal framework within that jurisdiction and is outlined in Annex i.

Northern Ireland

1.13 The DNA profiles from Northern Ireland relating to records where there has not been a positive match within the NI Database are submitted to the NDNAD for storing and matching. Retention of the records has to comply with the legal framework within that jurisdiction and are outlined in Annex i.

Other uses of DNA

1.14 There is no mandatory requirement to provide DNA to support an immigration application, however it can be accepted as evidence of a genetic relationship between individuals when this is generic to the application and the applicant is unable to provide that evidence from other acceptable sources. The Home Office does not take the DNA for the test; this is arranged by the applicant. The DNA test may only be conducted through an approved DNA testing company which meets the standards required (ISO17025). The Home Office receives the outcome of the result – not the DNA sample or profile.

Facial images

1.15 Facial images are collected by HM Passport Office, UK Visas and Immigration and Border Force and used in a number of ways across UK Government for issuing documents of entitlement, the assurance of identity and in the control of migration. The police services of England and Wales also take facial images under powers set out in PACE (s.64A). These are used in the investigation and prevention of crime and terrorist activities. Police also use facial images for public protection (e.g. finding Missing Persons)

1.16 HMPO collects a facial image which is stored on HMPO Main Index as part of their business process[7]. These are used to aid the decision-making process on an application for a British passport and the issuance of passports and other travel documents. With the applicant's consent they can provide images to DVLA for driving licences.

Official – sensitive: start of section

1.17 The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

1.18 Border Force checks facial images against the image contained in the travel document at the Primary Control Point (PCP), at e-gates[8] and via Vision Box (which provides, at the PCP, the same checking functionality as e-gates[9]). Border Force officers can use immigration powers[10] in certain circumstances to collect a face image as part of the fingerprint enrolment process. This image is stored in IABS

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286301/Privacy_Policy_28.2.14.pdf

[8] ePassport gates use facial recognition technology to verify the user's identity against the data stored in the chip in their biometric passport

[9] these image are not centrally stored

[10] Under the 1971 Act and the Immigration and Asylum Act 1999.

1.19 UKVI collect a facial image as part of their standard business processes, for example, as part of an asylum claim, a visa / entry clearance or Biometric Residence Permit (BRP) application. These are stored in IABS.

1.20 Facial images (and fingerprints) are captured from individuals who apply to become British citizens and stored on IABS. A photograph is also stored on the Case Information Database (CID)[11]. When the individual becomes a British citizen, their fingerprints and facial image are deleted from IABS, but the photograph on CID is retained until the individual obtains a British passport.

1.21 Immigration Enforcement collect facial images when serving removal directions and from asylum applicants (and their dependents). These are stored on IABS.

1.22 Police forces collect facial images as part of the custody process which are stored locally, some of which are uploaded onto the PND to provide a background gallery of people known to the police. Police Officers are then able to use other images of unknown individuals, and search this database to provide a lead to aid their work.

The face recognition system does not identify criminals, it is a tool to improve the human's efficiency, and record keeping.

Recognition from facial images is not forensic science, and automatically generated match scores (on their own) would not constitute an expert or forensic science or form a "lights out" process. [12]

Custody images are held on PND and from 2017 form part of the HOB programme scope[13] – a Custody Image Review was published 24 February 2017 https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

[11] CID is the Home Office's main caseworking and operational database. It is used throughout the Home Office to record personal details of all foreign nationals who pass through the Immigration system

[12] Forensic Image Comparison and Interpretation Evidence: Guidance for Prosecutors and Investigators https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/511168/Image_Comparison_and_Interpretation_Guidance_Issue_2.pdf

[13] HOB Project - Facial Images for Law Enforcement purposes

1.23 Retention: For immigration purposes the retention of facial images is as set out under regulations, made under the Immigration Act 2014. In general, facial images are retained until the person becomes a British Citizen and obtains a British passport.

1.24 The regime governing the retention of custody images is set out in the Code of Practice on the Management of Police Information ('MOPI') and guidance contained in the College of Policing Authorised Professional Practice ('the APP'). The Home Office made recommendations for changes to this regime in the Custody Images Review, which was published on 24 February 2017 which were implemented by changes to MOPI and the APP.

Fingerprints

1.25 There are two different methods of taking fingerprints:

Plain impression[14]: The friction ridge detail is recorded by being placed straight down onto a surface, without any rolling. For policing purposes, these impressions are primarily taken to ensure that the rolled impressions have been taken in the correct order on the fingerprint form. They can also be very useful in providing extra information to the Fingerprint Examiner, which may have been missed or poorly recorded when taking the rolled impressions. For immigration purposes, they are the method for fingerprint capture for applications made for visas and BRPs. Rolled fingerprints are taken in connection with claims for asylum or following the arrest of an illegal migrant.

Rolled impression: The friction ridge detail is recorded by rolling the digit to capture the maximum surface of the friction ridge skin. When completing a rolled impression of a finger, the whole pad of the finger should be rolled across the surface, i.e. from nail edge to nail edge. The sides of palm can be rolled to capture the detail there.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

[14] Frequently referred to as flat

Official – sensitive: end of section

1.26 In addition to fingerprints, palm prints may be taken:

Palm print: An impression of the friction ridges of all or any part of the palm surface of the hand, taken under controlled conditions.

Fingerprint process:

1.27 UKVI collects plain impressions for visa / entry clearance & BRP applications and rolled impressions for asylum enrolment. These are submitted to IABS for either a one-to-one check against previously enrolled fingerprints (1:1) to verify identity or a one-to-many search for a match within a defined fingerprint collection (1:M/N) or a combination of both. Biographic data is stored on IABS and the fingerprints are searched against IDENT1. Additionally, for asylum enrolment, rolled fingerprints are searched against Eurodac[15], the European fingerprint database for identifying asylum seekers and irregular border-crossers

1.28 Border Force uses index finger and thumb prints as part of the secureID (search only) check. These prints are used for a 1:1 check against the print enrolled at the time of visa / entry clearance application. If no match is returned a 1:N search is performed against the full IABS dataset.

1.29 Border Force collects both rolled and plain (flat) fingerprints as part of the asylum enrolment process, and for further purposes, for example as confirmation of identity. Discretionary searches can be undertaken on either IDENT1 or Eurodac, dependant on the reason for fingerprinting. For asylum cases IDENT1 and Eurodac checks are mandatory. Limited biographic data is stored with the fingerprint data.

1.30 Immigration Enforcement have an enrolment capability, (and includes checks against IDENT1) they also use fingerprints to check basic biographical background information from IABS. They can check fingerprints in the field using a mobile device (RapID[16]) which searches against immigration sets.

[15] Which stands for European Dactyloscopy

[16] To be replaced by Strategic Mobile

1.31 Police collect both rolled and plain tenprints along with palm prints, the sides of palms and upper palms at a custody suite using a Livescan3 unit. They can check index finger prints in the field using a Strategic Mobile device if a person is suspected of committing an offence and providing false information about their identity. Strategic Mobile searches policing and immigration sets.

1.32 The police,[17] and NCA collect latent prints lifted from a crime scene to match against individuals and latents already held on IDENT1 under s.61 of PACE

1.33 Retention: For immigration, the retention of fingerprint biometrics is as set out under regulations, made under the Immigration Act 2014. In general, fingerprints are retained for up to 10 years except in certain specified circumstances, with the exception of fingerprints taken under the 1999 Act. For policing, the Protection of Freedoms Act 2012 (POFA), which amended PACE, established a new regime to govern the retention and use of fingerprints taken by the police in England & Wales. The provisions are summarised in Annex i and also the provisions for retaining fingerprints in Scotland and Northern Ireland.

Scope of HOB

1.34 The HOB programme will replace existing systems. The new functionality being delivered does not involve the collection of additional data about individuals. Any changes in HOB scope will require an update to the HOB PIA.

Will the project compel individuals to provide information about themselves?

No

Current Situation

Policing

2.1 The Police and Criminal Evidence Act 1984 (PACE) and the accompanying PACE Codes of Practice[18], establish the powers of the police, in

[17] MoD also collect prints in connection with their military police duties, and also from IEDS in theatre in conflicts

[18] https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

England and Wales, to combat crimes while protecting the rights of the public. Code D (2017) concerns the principle methods used by police to identify people in connection with the investigation of offences and the keeping of accurate and reliable criminal records. HOB is the data processor for some of the activities.

- Fingerprints & Fingerprinting

2.2 Identification by fingerprints applies when a person's fingerprints are taken to: compare with fingerprint marks found at the scene of a crime, check and prove convictions or to help or to ascertain a person's identity.

Powers for taking fingerprints in connection with a criminal investigation is in Code D (2017) section 4.

  - 4.2 A person's fingerprints may be taken in connection with the investigation of an offence only with their consent or if paragraph 4.3 applies. If the person is at a police station, consent must be in writing.
  - 4.3 PACE, s.61, provides powers to take fingerprints without consent from any person aged ten or over

2.3. Within 4.3 the circumstances under which a person's fingerprints may be taken are laid out; the main powers for police are those that arise after arrest for a recordable offence[19] (PACE s.61.3); charged with a recordable offence (PACE s.61.4) or from a person who has been bailed to appear at a court or police station (PACE s.61(4A)),

2.4 Use of mobile devices. The power under s.61(6A) of PACE described in paragraph 4.3(e) allows fingerprints of a suspect who has not been arrested, and whose name is not known or cannot be ascertained, or who gave a doubtful name, to be taken in connection with any offence (whether recordable or not) using a mobile device and then checked on the street against the database containing the national fingerprint collection. Fingerprints taken under this cannot be retained after they have been checked

[19] References to 'recordable offences' in this Code relate to those offences for which convictions or cautions may be recorded in national police records. See PACE, s.27(4).

2.5. 4B of Code D sets out the circumstances under which fingerprints or a DNA sample may be checked against other fingerprints, and DNA records held by, or on behalf of, the police and other law enforcement authorities in, or outside, the UK, or held in connection with, or as a result of, an investigation of an offence inside or outside the UK. These powers arise when a person is arrested on suspicion of being involved in a recordable offence, or charged with a recordable offence.

- Photographs

2.6 Taking photographs of arrested people applies to recording and checking identity and locating and tracing persons who are wanted for offences or fail to answer their bail

2.7 Examinations to establish identity and the taking of photographs is covered in Code D, section 5, para 5.12 – 5.18 refer. The power to take photographs with or without consent is covered in 5.12

  - 5.12A Photographs taken under PACE, s.64A: (a) may be taken with the person's consent, or without their consent if consent is withheld or it is not practicable to obtain their consent, see Note 5E; and (b) may be used or disclosed only for purposes related to the prevention or detection of crime, the investigation of offences or the conduct of prosecutions by, or on behalf of, police or other law enforcement and prosecuting authorities inside and outside the United Kingdom or the enforcement of any sentence or order made by a court when dealing with an offence. After being so used or disclosed, they may be retained but can only be used or disclosed for the same purposes.

- DNA identification

2.8 Section 6 of Code D (2017) Covers identification by body samples and impressions including taking samples such as a cheek swab, hair or blood to generate a DNA profile for comparison with material obtained from the scene of a crime, or a victim. The main powers for taking DNA arise after arrest for a recordable offence

  - 6.1 References to:

(a) an "intimate sample" means

a dental impression or sample of blood, semen or any other tissue fluid, urine, or pubic hair, or a swab taken from any part of a person's genitals or from a person's body orifice other than the mouth;

(b) a "non-intimate sample" means:

(i) a sample of hair, other than pubic hair, which includes hair plucked with the root,

(ii) a sample taken from a nail or from under a nail;

(iii) a swab taken from any part of a person's body other than a part from which a swab taken would be an intimate sample;

(iv) saliva;

(v) a skin impression which means any record, other than a fingerprint, which is a record, in any form and produced by any method, of the skin pattern and other physical characteristics or features of the whole, or any part of, a person's foot or of any other part of their body.

2.9 Code D (2017) 6.5 -6.9 covers the circumstances under which non-intimate sample may be taken either with written consent or with the reasonable use of force from a detainee only with their written consent or if paragraph 6.6 applies.

Immigration and Asylum

2.10 An authorised person can compel an individual to provide fingerprints when they claim asylum, arrive at the border undocumented, are arrested or detained under immigration powers, are granted immigration bail[20], or are subject to removal and deportation, and the dependants of individuals in these categories under s.141 of the Immigration and Asylum Act 1999. These can be compelled using reasonable force if the claimant is refusing to provide the information under s.146(2) of the Immigration and Asylum Act 1999.

[20] The immigration bail provisions in the 2016 Act commenced on 15th January 2018

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

2.12 s.126 of the Nationality, Immigration and Asylum Act 2002 allows the Secretary of State to make regulations requiring a person making an immigration application to provide biometric information[21]. This was used to make The Immigration (Provision of Physical Data) Regulations 2006, as amended.

2.13 An authorised person can require an individual to provide biometric information to apply for a document, recording biometric information under the regulations in the Immigration (Biometric Registration) Regulations 2008, as amended, which detail the process by which a person's fingerprints and photograph may be obtained and recorded.

2.14 Regulation 9 of the above provides that the Secretary of State may use a record of a person's fingerprints or a photograph of a person's face in accordance with the following purposes:

- In connection with the exercise of a function by virtue of the Immigration Acts
- In connection with the control of the United Kingdom's borders
- In connection with the exercise of a function related to nationality
- In connection with the prevention, investigation, or prosecution of an offence
- For a purpose which appears to the Secretary of State to be required in order to protect national security
- In connection with identifying victims of an event or situation which has caused loss of human life or human illness or injury
- For the purpose of ascertaining whether any person has failed to comply with the law or has gained, or sought to gain, a benefit or service, or has asserted an entitlement, to which he is not by law entitled

2.15 Any changes in HOB scope will require an update to the HOB PIA.

[21] Defined by s15 of the UK Borders Act 2007, as amended.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Not at present

Current Situation

3.1 The Home Office has a "Personal Information Charter" which explains how personal information is looked after and shared[22].

Physical and logical security arrangements

3.2 All staff require the appropriate level of security clearance and training to gain access to Home Office buildings and systems

3.3 All HOB personnel receive security awareness training as part of their induction, both civil servants and contractors. All users must read and accept the POISE security operating procedures when first logging onto their account. The Department provides ongoing reinforcement training. Police users are subject to Information Security (IS) awareness regime in their individual forces.

3.4 All transactions are monitored and recorded. Protective monitoring is ongoing and includes records of all access – both successful and failures.

NDNAD[23] [24]

3.5 Day-to-day operation of the NDNAD service is the responsibility of the Home Office FINDS Unit.

3.6 A small number of staff have role-defined access to the NDNAD. Access is regularly reviewed.

3.7 No police officer or police force has direct access to the information held on the NDNAD but they are informed of matches that are generated.

[22] https://www.gov.uk/government/organisations/home-office/about/personal-information-charter
[23] https://www.gov.uk/government/publications/national-dna-database-annual-report-2013-to-2014
[24] https://www.gov.uk/government/publications/access-and-use-of-dna-samples-profiles-and-associated-data

3.8 Similarly, Forensic Science Providers (FSPs), who undertake DNA profiling under contract to the police service and submit the resulting crime scene and subject profiles for loading, do not have direct access to the information.

3.9 Members of the public may request access to a NDNAD record directly relating to them through a subject access request via the force who took their samples.

HMPO Facial Images

3.10 A number of organisations have access, by specified staff, to the data validation application which gives access to HMPO facial images

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

- ACRO Criminal Records Office
- Cabinet Office
- Crown Dependencies
- Disclosure and Barring Service (DBS)
- Driver and Vehicle Licensing Agency (DVLA)
- Department for Work and Pensions (DWP) - FES CCIS
- Financial Conduct Authority (FCA)
- Foreign and Commonwealth Office (FCO)
- Her Majesty's Revenue and Customs (HMRC)
- Home Office Immigration; Border Force, UKVI & ICE
- National Crime Agency (NCA)
- Police forces in England, Wales, Scotland and Northern Ireland - Serious Fraud Office (SFO)

- Security Industry Authority (SIA)
- Student Loans Company (SLC)
- HM Land Registry
- Environment Agency

IABS

3.11 IABS is used within HO processes primarily for immigration purposes and law enforcement. At a high level IABS connects to:

- FCOS and supporting UKVI services (visas etc.)
- Home Office Immigration; Border Force, UKVI & ICE
- IPT (BRP)
- HMPO
- IFB (checks)
- Policing via IDENT1 PIFE link (now provided via the Biometric Services Gateway)
- IDSC[25]
- EURODAC
- IVACs [26](Irish Visas).

3.12 Fingerprints enrolled in IABS are checked against existing prints held in IABS.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

3.13 Fingerprints enrolled on IABS relating to individuals who have claimed asylum in the UK or who have been detected in connection with an irregular crossing of the

[25] Five Country Conference – UK, USA, Canada, Australia and New Zealand
[26] Acting on behalf of the Irish authorities – effectively a visa application centre service for the Irish

border of the European Union or are illegally present in the UK are also sent to the EU's Eurodac database. Eurodac is a central store of fingerprints to allow the effective operation of the Dublin Regulation permitting asylum seekers to be returned to the first country of claim with-in the EU and the four Associated States (Iceland, Liechtenstein, Norway and Switzerland)

IDENT1[27]

3.14 IDENT1 Standard Bureau Services cover:

- All police forces in England, Wales, Northern Ireland & Scotland
- Specialist bureaux within law enforcement and government agencies including:
  - National Fingerprint Office (NFO)
  - Counter Terrorist Forensic Service (CTFS),
  - International Law Enforcement (via requests made to the National Crime Agency)
  - Ministry of Defence (MoD)
  - NCA
  - HMRC
  - IDENT1 Training Suites
- Government agencies and Crown dependencies which do not have their own bureau have made arrangements to use a specific force's bureau. These include:
  - DWP
  - Royal Mail Investigations
  - RAF Police
  - Isle of Man

[27] Identification Portfolio Service Catalogue 2014-15

- Jersey
- Guernsey

Connectivity with IABS:

- IDENT1 PIFE Interface Service (now provided via the Biometric Services Gateway)
  - UKVI
  - All police forces
- Other organisations which have access to IDENT1
  - ACRO

HOB Scope

3.15 The Biometrics Services Gateway (BSG) provides a new front door to the IABS and IDENT1. The gateway allows new capabilities to be delivered and will allow for the consolidation of services. This changes the way in which the information about individuals is accessed, and provides a system which will make it easier in future for groups that have not previously had routine access to the information to gain access if necessary – i.e. based on the requirement for access to the system being lawful, appropriate, proportionate and approved through the relevant governance board structure**. The HOB PIA will consider the privacy impact of this change.**

Future Scope

3.18 Several of the programme deliverables aim to enable greater data sharing between both government departments, and between countries.

3.19 The project also aims to make the different databases more readily accessible, for example the fingerprint databases.

3.20 Any changes in HOB scope will require an update to the HOB PIA.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Yes

Current Situation

4.1 Please see Question 0 “Will the project involve the collection of new information about individuals?” for the purpose the information is collected for.

HOB Scope

4.2 Generally, where the technology being delivered will allow for current operations to be done more efficiently, rather than introducing new capabilities, there will be no change in how the information is used.

4.3 In addition to replacing or updating the existing biometrics systems, some new functionality is being introduced.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

4.4 Any changes in HOB scope will require an update to the HOB PIA.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Yes

Current Situation

5.1 Consideration is given at all times to relevant legal requirements such as the ECHR and DPA in particular. The systems being replaced hold biometric information

which is sensitive personal data about individuals, *all* of which could be privacy intrusive, and *some* of which the individual can be compelled to supply.

HOB Scope

5.2 Generally, where the technology being delivered will allow for current operations to be done more efficiently, rather than introducing new capabilities, there will be no change in how intrusive the technology is perceived to be.

5.3 In addition to replacing or updating the existing biometrics systems, some new functionality has been introduced; automated 1:1 facial matching is applied to every adult passport application. The functionality is being extended to 1:M which will allow facial matching against the full database.

5.4 Business processes are not being changed by the programme and so changes to how the technology is used and thus changes to how intrusive its use is are not in the scope of the HOB programme.

5.5 There are however some areas where additional functionality will be made available to operational staff through future changes to existing technology. Access to limited IABS data will become available to police officers through their mobile devices. Also the searching of latent marks against immigration data became available to specialist bureaux in April 2018, replacing the largely manual process with an automated search, where specialist bureaux are now able to launch searches directly from IDENT1 to IABS, and receive the search results directly back.

5.6 Any changes in HOB scope will require an update to the HOB PIA.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Yes

Current Situation

6.1 DNA is used for identification purposes, to link a suspect to a crime scene sample, and to identify links between crime scenes.

6.2 Fingerprints are used for identification purposes, to link a suspect with a crime scene mark, and to identify links between crime scenes.

6.3 Fingerprints and face images are used to make a decision whether to grant visa / entry clearance, and whether to grant a BRP.

Official – sensitive: start of section

6.4 The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

6.5 Facial Images are used to verify and confirm entitlement or identify offenders and to link a suspect to a crime

HOB Scope

6.6 The technology being delivered is intended to allow for current operations to be done more efficiently as opposed to introducing new capabilities; as a result of which enhanced decision making should follow.

Official – sensitive: start of section

6.7 The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

6.8 Business processes are not being changed by the programme, and so changes to the decisions made or the actions taken are not in the scope of the HOB programme.

6.9 There are however some areas where additional functionality will be made available to operational staff through future changes to existing technology. Access to limited IABS data has become available to police officers through their mobile devices. Also the routine searching of latent marks against immigration data has become available to specialist police bureaux in 2018, replacing the largely manual,

adhoc, process with an automated search, where Police bureaux are now able to launch searches directly from IDENT1 to IABS, and receive the search results directly back.

6.10 Any changes in HOB scope will require an update to the HOB PIA.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Yes

7.1 Biometric information is sensitive personal data and it is recognised that criminal records are afforded additional protection in the DPA and this will be reflected in the technical and business architecture.

Will the project require you to contact individuals in ways that they may find intrusive?

No.

Annex i: Retention of DNA and Fingerprints

England and Wales[28]

Convictions

Situation	Fingerprint and DNA Retention
Any age convicted (including given a caution or youth caution) of a qualifying[29] offence	Indefinite
Adult convicted (including given a caution) of a recordable[30] offence	Indefinite
Under 18 convicted (including given a youth caution) of a recordable offence (which is not a qualifying offence)	1st conviction: 5 years (plus length of any prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Non-convictions

Situation	Fingerprint and DNA Retention
Any age charged with but not convicted of a qualifying offence	3 years plus a 2 year extension if granted by a District Judge (or indefinite if the individual

[28] This table does not include the Terrorism Act 2000 retention periods.
[29] A 'qualifying' offence is one listed under s.65A of the Police and Criminal Evidence Act 1984 (the list comprises sexual, violent, terrorism and burglary offences).
[30] A 'recordable' offence is one for which the police are required to keep a record. Generally speaking, these are imprisonable offences; however, it also includes a number of non-imprisonable offences such as begging and taxi touting. The police are not able to take or retain the DNA or fingerprints of an individual who is arrested for an offence which is not recordable.

Situation	Fingerprint and DNA Retention
	has a previous conviction for a recordable offence which is not excluded[31])
Any age arrested for but not charged with a qualifying offence	3 years if granted by the Biometrics Commissioner plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested and subject to a National Security Determination	2 year extension on first and any subsequent determination
Any age arrested for or charged with a recordable offence (which is not a qualifying offence)	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Adult given a Penalty Notice for Disorder	2 years
Any age arrested for recordable offence – case not concluded	Until case is concluded

Scotland[32]

[31] An 'Excluded' offence is a recordable offence which is minor, was committed when the individual was under 18, for which they received a sentence of fewer than 5 years imprisonment and is the only recordable offence for which the person has been convicted.

Convictions

Situation	Fingerprint and DNA Retention
Person[33] convicted of an offence	Indefinite

Non-convictions

Situation	Fingerprint and DNA Retention
Person subject to criminal proceedings for relevant sexual or violent offence[34]	3 years following conclusion of proceedings, plus a 2 year extension(s) if granted by a Sheriff[35]
Person offered an alternative to prosecution[36] for an offence that is not a relevant sexual or violent offence	2 years plus a 2 year extension(s) if granted by a Sheriff[37]
Person offered alternative to prosecution for an offence that is a relevant sexual offence or violent offence.[38]	3 years plus a 2 year extension(s) if granted by a Sheriff[39]

[32] Retention rules are set out in Part 2 of the Criminal Procedure (Scotland) Act 1995. S.18(3) outlines a general rule of destruction of samples following a decision not to institute criminal proceedings or when proceedings do not end with conviction, exceptions to the general rule are found within ss.18A to 18G of the 1995 Act.
[33] This may (rarely) include children. Part 5 of the 1995 Act deals with the criminal justice treatment of children and young people. The age of criminal responsibility in Scotland is 8 (s.41) though no child under 12 may be prosecuted (s.41A) and children under 16 may only be prosecuted on the instruction of the Lord Advocate (s.42). In practice children under 16 are not usually prosecuted and offending behaviour is dealt with instead by way of referral to the children's hearing system.
[34] These terms are defined in s.19A (6) of the 1995 Act.
[35] s.18A of the 1995 Act.
[36] Prosecutors may offer a fixed penalty, compensation offer or work order – see ss.302 to 303ZB of the 1995 Act.
[37] s.18B of the 1995 Act.
[38] The list of relevant sexual and relevant violent offences is set out in s.19A (6) of the 1995 Act.
[39] s.18C of the 1995 Act.

Situation	Fingerprint and DNA Retention
Person arrested and subject to a national security determination	2 years and may be renewed by any subsequent determination[40]
Person subject to certain fixed penalty notices[41]	2 years[42]
Child referred to a children's hearing on grounds of having committed a relevant sexual or violent offence[43]	3 years[44], with two year extensions if granted by a Sheriff[45]

Northern Ireland[46]

Convictions

Situation	Fingerprint and DNA Retention
Any age convicted (including given a caution or youth caution) of a qualifying offence	Indefinite
Adult convicted (including given a caution) of a recordable offence	Indefinite

[40] s.18G of the Criminal Procedure (Scotland) Act 1995.
[41] This covers fixed penalty notices issued by a police constable under s.129 of the Antisocial Behaviour (Scotland) Act 2004 for antisocial behaviour offences relating to drunkenness, vandalism, breach of the peace, etc.
[42] s.18D of the 1995 Act.
[43] For the purposes of s.18E of the 1995 Act, the relevant sexual or violent offences are set out in a statutory instrument, the Retention of Samples etc. (Children's Hearings) (Scotland) Order 2011 (SSI 2011/197).
[44] s.18E of the 1995 Act.
[45] s.18F of the 1995 Act.
[46] At the time of writing the Northern Ireland retention rules in Schedule 2 of the Criminal Justice Act (Northern Ireland) have yet to be commenced.

Situation	Fingerprint and DNA Retention
Under 18 convicted (including given a youth caution) of a recordable offence (which is not a qualifying offence)	1st conviction: 5 years (plus length of any prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Non-convictions

Situation	Fingerprint and DNA Retention
Any age charged with but not convicted of a qualifying offence	3 years plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for but not charged with a qualifying offence	None[47]
Any age arrested and subject to a National Security Determination	2 year extension on first and any subsequent determination.
Any age arrested for or charged with a recordable offence (which is not a qualifying offence)	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)

[47] [1] Article 63D(5)(c), 63D(11) to (13) and the definition of prescribed in Article 63D(14) of PACE NI make provision for material from persons arrested but not charged with a qualifying offence to be retained for 3 years if granted by the NI Biometric Commissioner plus a further 2 years if granted by a District Judge. At the time of writing these provisions have not been commenced and are unlikely to be for the foreseeable future.

Situation	Fingerprint and DNA Retention
Adult given a Penalty Notice for Disorder	2 years
Any age arrested and DNA/FP taken but case not concluded	Until case is concluded

Annex ii: Contributors

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section