

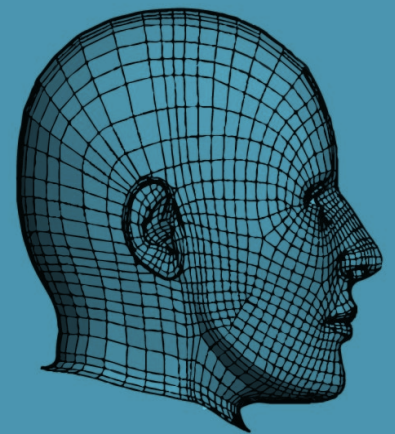
---

HM INSPECTORATE OF CONSTABULARY IN SCOTLAND

# **Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland**

January 2016

---





---

© Crown copyright 2016

Produced and Published by Her Majesty's Inspectorate of Constabulary in Scotland (HMICS)

ISBN: 978-1-910165-25-6

Laid before the Scottish Parliament by Her Majesty's Inspector of Constabulary in Scotland under section 79(3) of the Police and Fire Reform (Scotland) Act 2012

HMICS/2016/01

[www.hmics.org.uk](http://www.hmics.org.uk)

---

# HM Inspector of Constabulary in Scotland

---

HM Inspectorate of Constabulary in Scotland (HMICS) is established under the Police and Fire Reform (Scotland) Act 2012 (the Act) and has wide-ranging powers to look into the 'state, effectiveness and efficiency' of both the Police Service of Scotland (Police Scotland) and the Scottish Police Authority (SPA).<sup>1</sup>

We have a statutory duty to ensure that the Chief Constable and the Authority meet their obligations in terms of best value and continuous improvement. If necessary, we can be directed by Scottish Ministers to look into anything relating to the Authority or Police Scotland as they consider appropriate. We also have an established role in providing professional advice and guidance on policing in Scotland.

- Our powers allow us to do anything we consider necessary or expedient for the purposes of, or in connection with, the carrying out of our functions.
- The Authority and the Chief Constable must provide us with such assistance and co-operation as we may require to enable us to carry out our functions.
- When we publish a report, the Authority and the Chief Constable must also consider what we have found and take such measures, if any, as they think fit.
- Where our report identifies that the SPA or Police Scotland is not efficient or effective (or best value not secured), or will, unless remedial measures are taken, cease to be efficient or effective, Scottish Ministers may direct the Authority to take such measures as may be required. The SPA must comply with any direction given.
- Where we make recommendations, we will follow them up and report publicly on progress.
- We will identify good practice that can be applied across Scotland.
- We work with other inspectorates and agencies across the public sector and co-ordinate our activities to reduce the burden of inspection and avoid unnecessary duplication.
- We aim to add value and strengthen public confidence in Scottish policing and will do this through independent scrutiny and objective, evidence-led reporting about what we find.

Our approach is to support Police Scotland and the Authority to deliver services that are high quality, continually improving, effective and responsive to local needs.<sup>2</sup>

**This audit and assurance review was undertaken by HMICS in terms of Section 74(2) (a) of the Police and Fire Reform (Scotland) Act 2012 and laid before the Scottish Parliament in terms of Section 79(3) of the Act.**

---

<sup>1</sup> Police and Fire Reform (Scotland) Act 2012, Chapter 11.

<sup>2</sup> HMICS, *Corporate Strategy 2014-17*.

# Contents

---

	<b>Page</b>
Our inspection	3
Key facts	5
Key findings	8
Recommendations	9
Background and methodology	10
The statutory framework for the police use of images and biometric samples in Scotland	14
Police Scotland policy and practice in relation to the Criminal History System (CHS) and the UK Police Database (PND)	21
Findings from our audit and review of use of the facial search functionality within PND by Police Scotland	23
Governance arrangements for PND	29
Administrative and technical interfaces between Police Scotland CHS and the UK PND including weeding and retention of images	34
Comparisons with England and Wales	37
The future direction of biometrics	43
<b>Appendix 1:</b> Basic overview of biometric sample journey within the wider Criminal Justice Process in Scotland.	45
<b>Appendix 2:</b> Basic Process Map showing technical and administrative interface between CHS and PND in Scotland	46
<b>Appendix 3:</b> Glossary	47

## Our inspection

---

The aim of this audit and assurance review is to consider the state, effectiveness and efficiency of the arrangements surrounding the use by Police Scotland of the facial search technology capabilities contained within the UK Police National Database (PND). In doing so, we also consider the statutory framework that underpins the police use of biometric data in Scotland. It should be noted at the outset that we use the term 'facial search' and not facial recognition as police images in the Criminal History System (CHS) in Scotland, and those in the broader UK PND system, are not of sufficient digital resolution for them to be used against software that would deliver a true automated recognition capability. In other words, PND does not deliver a facial recognition capability, but instead returns a list of potential image matches that then require further human assessment and investigation.

The audit and assurance review follows on from questions directed to the Scottish Government in 2015 relative to the police use of facial recognition technologies in Scotland.<sup>3</sup> It also takes cognisance of a request from the Cabinet Secretary for Justice for HMICS to consider including scrutiny of this area in our programme of work for 2015/16.<sup>4</sup>

As part of this audit and assurance review, we have examined Police Scotland's current practice and have assessed compliance with internal policy. We have also reviewed governance and oversight arrangements within Police Scotland including the administrative and technical interface between CHS and the wider UK PND with regard to the recording, weeding and retention of information by Police Scotland. This has included a review of how Police Scotland interfaces with wider UK governance arrangements around PND, and how the arrangements in Scotland align with current statutory PND Codes of Practice for England and Wales.

For completeness, our audit and assurance review also provides comparisons with the legislative approaches to biometric data retention in England and Wales. It also considers the use of the PND and other facial search software adopted by forces in England and Wales, and considers the wider policing and societal opportunities and threats which arise from the police use of such new and emerging biometric technologies.

This audit and assurance review was conducted as part of our scrutiny programme for 2015/16. Our programme provides flexibility to scrutinise new and emerging issues affecting

---

<sup>3</sup> *Motion S4M-12676: Alison McInnes, North East Scotland, Scottish Liberal Democrats, Date Lodged: 16/03/2015 Police use of Images with Facial Recognition Technology*: 'That the Parliament understands that police forces from across the UK have uploaded up to 18 million photographs to the Police National Database for use with facial recognition technology; is concerned that these images might include those of people never charged with an offence or who have been found innocent of a crime; notes the statement by the Chief Constable of Durham Constabulary on Newsnight on 2 February 2015 that, in a recent case in his constabulary, a person was identified using photographs from Scotland; further notes the concerns of the Biometrics Commissioner, Alastair MacGregor QC, regarding the implications for civil liberties of the use of such technology; notes his comment that "urgent steps" should be taken to ensure that facial recognition and other biometric technologies should be governed by an appropriate regulatory regime; considers that, although facial recognition technology might be a useful policing tool, such technology must only be used with suitable safeguards and protection for innocent members of the public; believes that Police Scotland's use of, or contribution of images to, the Police National Database, or any other database for facial recognition purposes, should be in the context of specific laws set by the Parliament, and considers that legislation similar to that agreed by the Parliament to govern the use of DNA profiles and fingerprints should be adopted to regulate the police use of images for facial recognition purposes and that police use of any new biometric identification technology in the future should be subject to similar regulation'.

<sup>4</sup> Letter to HMICS dated 22 June 2015.

policing in Scotland. These issues are identified through a process of stakeholder engagement and are informed by our scrutiny risk assessment. Our work is based on our HMICS Inspection Framework which ensures a consistent and objective approach to our work.

The HMICS framework considers six overarching themes, namely:

- Outcomes
- Leadership and Governance
- Planning and Process
- People
- Resources
- Partnerships



As a consequence of our audit and assurance review, Police Scotland and the Scottish Police Authority will be asked to create an action plan, so that our recommendations are taken forward to enable relevant good practice to be disseminated across Scotland to promote continuous improvement. We will monitor progress against this plan and publish our findings as part of our annual reporting process.

HMICS wishes to thank Police Scotland and the Scottish Police Authority and the many officers and members of staff who participated in our audit and assurance review. Particular thanks are due to Detective Chief Inspector Russell Penman from Police Scotland, Mr Tom Nelson, Director of Forensic Services with the Scottish Police Authority, Mr Alastair MacGregor QC, Biometrics Commissioner for England and Wales and Mr Sean Byron, National Business Change Manager for PND systems within the Home Office.

Our Audit and Assurance Review was conducted by Dr. Brian Plastow and Joanna Drapper, HMICS.

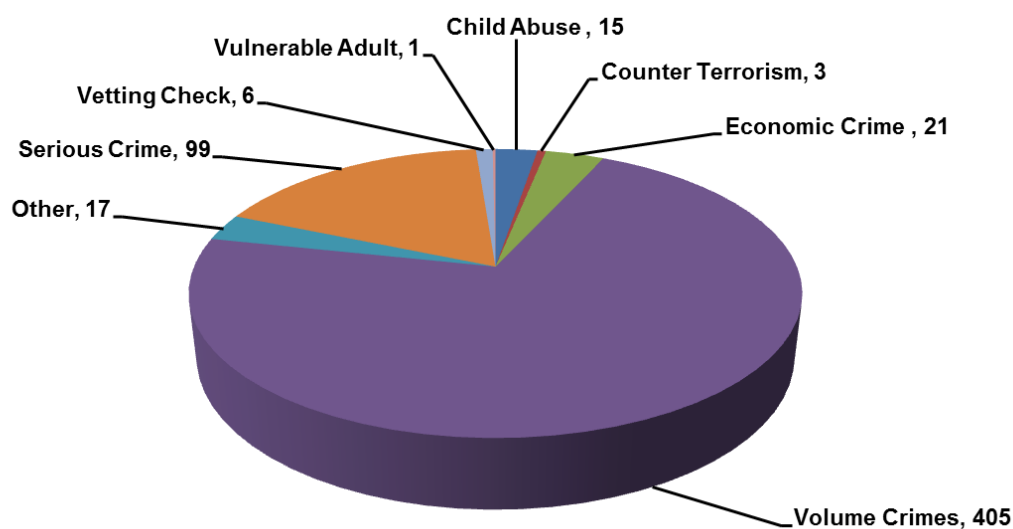
Executive lead was provided by the Assistant Inspector of Constabulary, Mr. Andy Cowie.

**Derek Penman QPM**  
HM Inspector of Constabulary in Scotland  
January 2016

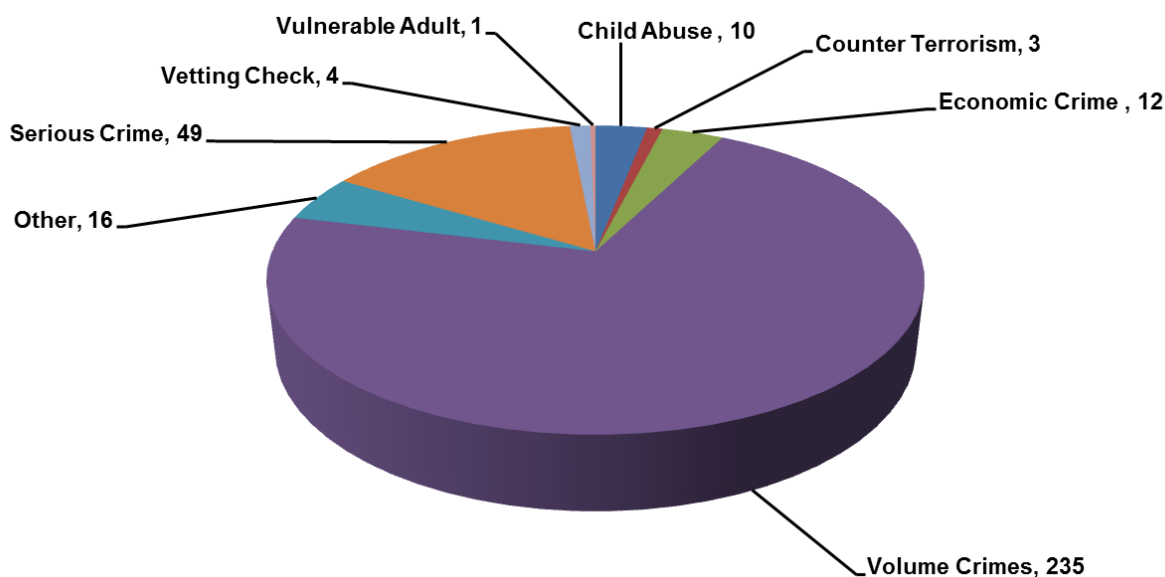


## Key facts – Analysis of the use of PND facial search by Police Scotland to 08 July 2015.<sup>5</sup>

567 Facial Searches by Police Scotland shown by PND Search Reason Codes<sup>6</sup>



The 567 Searches by Police Scotland were of 330 crime scene probe images which are shown below by PND Search Reason Codes



<sup>5</sup> See full details and findings of our audit on page 25 of this report.


<sup>6</sup> Volume crimes are recorded under a generic PND Search Reason Code 'Intelligence - level 2. However, we use the term volume crime in this report.

## Key facts

---

- The police use of biometrics is not a new phenomenon. The Police in Scotland have been using criminal history photographs and fingerprints for more than 100 years and DNA for more than 30 years. However, this is a fast and evolving area of law enforcement.
- The UK Police National Database (PND) Facial Search works by comparing an uploaded 'probe image' from a crime scene or incident, against a 'gallery image' previously placed on the PND intelligence sharing system from UK police records. When searched, the system returns a number of possible image matches which then require human assessment, comparison and investigation.
- Information on any potential match is passed to the relevant enquiry officer for further development of the intelligence product. The PND system does not therefore have a means of recording the number of successful identifications of suspects, and there has been no UK or Scottish evaluation of the reliability of the system in the live operational context.
- The UK PND was introduced in 2008 and all Scottish Criminal History (CHS) records were uploaded to PND in 2011. A criminal history image forms part of that record so all CHS images have also been present within PND since 2011. This means that other UK forces have been able to manually view individual Scottish Criminal History System (CHS) images since 2011.
- The operational introduction of PND in Scotland, and the upload of CHS records in 2011, was made by the former Association of Chief Police Officers in Scotland (ACPOS) and the former Scottish Police Services Authority (SPSA) under legacy policing arrangements. The key planning decisions in relation to placing Scottish CHS records and images on to the UK PND were made prior to the establishment of Police Scotland and the Scottish Police Authority. This included planning for the modular updates within PND such as the Facial Search capability.
- The Facial Search functionality of PND became generally available in March 2014, and at that time the Scottish CHS records contained 601,837 images of 334,594 people. There were 11.8 million images in PND meaning the Scottish CHS images accounted for 7.1% of the UK total.
- Scottish CHS records on PND contain images of persons who have been charged or convicted of an offence. This contrasts with approaches in England and Wales where it is custody images that are uploaded due to the absence of a unified criminal history system or any policy or guidance to the contrary.
- Police Scotland removes images of persons not subsequently convicted of a crime from CHS and PND. This process can take up to six months due to the need to weed all electronic and hard copy images and to physically destroy fingerprints and DNA samples. This manual processing is done in response to reports generated from the CHS system. This also caters for circumstances where an accused person is found not guilty of some charges but guilty of others and the complications of rolling and merging cases. In most cases, manual deletion of these materials takes place more quickly.



- 
- Whilst images of persons not convicted of a crime are removed from CHS, Police Scotland does retain the custody episode images for periods of either six or twelve years in accordance with data retention policies but these are not uploaded to PND. As with England and Wales, this includes images of persons who have not been charged with any crime or offence, and of people against whom no criminal proceedings have been taken.
  - Nine forces in England and Wales do not upload custody images to PND, and at least one force in England and Wales uses an additional facial search product.
  - Whilst Police Scotland maintains the Scottish Criminal History System (CHS), the Scottish DNA Database (SDNAD) and the Scottish fingerprint records on the UK Fingerprint Database (IDENT1) are maintained by the Scottish Police Authority in conjunction with Police Scotland.
  - The statutory framework in Scotland has specific legislation to govern and regulate the retention of biometrics such as fingerprints and DNA, but there is no similar legislation which specifically governs the police retention and use of photographic images. This is also the position in England and Wales as recently highlighted by the Biometrics Commissioner.
  - Different approaches are being taken to the uploading of images to the PND by forces throughout the UK. This means that differing standards are being applied to a common UK database.
  - There is no independent oversight of the police use of biometrics in Scotland as called for in the 2008 Fraser Report. This contrasts with the position in England and Wales where the Protection of Freedoms Act, 2012 introduced a new biometrics regime including the appointment of an independent Biometrics Commissioner for England and Wales.
  - There is a statutory Code of Practice on the Police Use of PND for England and Wales but this code had no statutory basis in Scotland.

## Key findings

---

- Police Scotland had conducted 567 facial searches on PND in the period from 28 March 2014 to 8 July 2015. These 567 searches were of 330 different probe images obtained from crime or incident scenes.
- The number of facial searches conducted on PND by Police Scotland is equivalent to less than one search per day. Our audit found that each search by Police Scotland related to a specific crime, incident or enquiry and all uses by Police Scotland were lawful, proportionate and necessary.
- Our audit of the use of PND found that Police Scotland was fully compliant with its own policy around the use of PND, and also with Home Office and College of Policing guidance.
- PND gives Police Scotland access to custody information from England, Wales and Northern Ireland from biometric records arising from circumstances where the retention of such information on PND would not have been permissible under current policy had the record been created in Scotland.
- Whilst we are satisfied from this review that Police Scotland has been making proportionate and necessary use of Facial Search within PND, we have also identified a need for improved legislation and better independent oversight around the police use of biometrics in Scotland.
- In contributing to UK policing systems, it is important that Police Scotland has the functionality to administer and maintain Scottish data in compliance with both Scottish legislation and any Scottish Codes of Practice in terms of its use.

# Recommendations

---

## **Recommendation 1**

Scottish Government should work with Police Scotland and the Scottish Police Authority to consider legislative provision in relation to the retention and use of photographic images by the police.

## **Recommendation 2**

Scottish Government should work with Police Scotland, the SPA, COPFS and other interested parties to consider the establishment of an independent Scottish Commissioner to address the issues of ethical and independent oversight over biometric databases and records held in Scotland, with sufficient flexibility to embrace future technologies and relevant codes of practice.

## **Recommendation 3**

Police Scotland should amend its internal PND Search Request Form so that the reasons for requested PND searches are coded to align directly with the PND Search Reason Codes in the live database.

## **Recommendation 4**

Police Scotland and the Scottish Police Authority should consult with Scottish Government and other stakeholders on the potential development of a statutory Code of Practice for the use of biometric data in Scotland.

# Background and methodology

---

## Background

### Police Scotland Criminal History System (CHS)

1. Police Scotland maintains a Criminal History System (CHS), where all records and images of charged and convicted persons are stored. The criminal history images within these records are derived from photographic images relating to a particular custody episode when an arrested or detained person is brought into police custody.
2. The criminal history records of persons charged or convicted with a common law crime or statutory offence in Scotland on CHS are automatically uploaded to a UK policing intelligence sharing system known as the Police National Database (PND) so that other UK forces can search the PND to help identify and prosecute criminals. In the event of acquittal, the records and images are removed from CHS and PND by Police Scotland once notified of non conviction or absolute discharge by the Crown Office and Procurator Fiscal Service (COPFS).
3. Police Scotland voluntarily applies similar policy to the retention and weeding of photographs on CHS as exists in primary Scottish legislation for fingerprints and DNA<sup>7</sup>. The primary legislation in Scotland does however allow the data from individuals prosecuted for certain sexual and violent offences to be retained for three years (whether or not they are convicted); with the Chief Constable able to apply to the Sheriff Court for further two year extensions.
4. The UK police force which places any record on PND is the record owner under PND business operation rules, it therefore follows that other records on PND from non Police Scotland sources are not weeded by Police Scotland.

### Police Custody Images in Scotland

5. Police custody episode images in Scotland are not uploaded to CHS and PND unless the subject has been charged with a crime or offence in which case they are uploaded as part of pending case data. This differs from the position in England and Wales where most forces upload all custody images directly to PND due to the absence of any single unified criminal history system or any statutory controls or guidance to the contrary.
6. However, Police Scotland does retain all custody images on legacy force custody systems in accordance with existing data retention policy for periods of either six or twelve years.<sup>8</sup> As with England and Wales, this includes images of persons who have not been charged with any crime or offence, and of people against whom no criminal proceedings have been taken. This contrasts with the approach taken in Scotland for fingerprints, DNA and the CHS images which are all destroyed if no proceedings are taken against the person to whom those various biometric records relate.
7. The reason that custody images are retained is to assist in the investigation of circumstances where arrested persons may have provided false identity details to the

---

<sup>7</sup> Images will be retained where the photograph is part of an on-going pending case and/or where the photograph is of the same date or newer than the oldest case which resulted in the conviction.

<sup>8</sup> The standard Police Scotland data retention policy is six plus one years and twelve for high tariff crimes or offences. The Police Scotland Record Retention SOP cites the Prescription and Limitation (Scotland) Act 1984 as a legal point of reference.

police or other circumstances such as retrospective complaints being made about a particular custody episode. Legacy force custody systems in Scotland are due to be replaced by a new integrated custody application under the Police Scotland i6 programme. At this juncture, Police Scotland will archive the data from the legacy force systems until destroyed at the conclusion of prescribed data retention periods.

### **UK Police National Database (PND)**

8. In 2002, two children, Holly Wells and Jessica Chapman, were murdered by school caretaker Ian Huntley. This led to a public inquiry led by Sir Michael (now Lord) Bichard and the publication in 2004 of the Bichard Inquiry Report.<sup>9</sup> The Bichard report noted that forces in England and Wales had no means of knowing what intelligence, if any, was held on any particular individual by another force and also that there was no information based technology way of finding out.<sup>10</sup> Bichard also found that the lack of shared intelligence systems in England and Wales compared unfavourably with the position in Scotland at the time which was in the final stages of implementation of the single Scottish Intelligence Database (SID).<sup>11</sup>
9. His primary recommendation was that an intelligence system for police forces in England and Wales should be introduced and that there was learning to be adopted from the approach in Scotland. If such a system had been in place, Huntley was likely to have been identified as a serious threat to children far sooner as he was already known to the police in England.
10. In 2008, the Home Office introduced the UK Police National Database (PND). The PND is a confidential and restricted UK data store of operational policing information and intelligence provided by individual forces and law enforcement agencies, including Police Scotland. It is not an evidential system. It contains copies of locally held police records covering intelligence, crime, custody, child and domestic abuse investigations. This includes facial images of people arrested or detained from police custody records in England, Wales and Northern Ireland, but as discussed above the images from Scotland come solely from the Scottish CHS introduced under legacy policing arrangements. Notably, nine forces in England and Wales do not yet upload custody images to PND and some like Leicestershire Police also have additional bespoke facial search technologies.<sup>12</sup>

### **Facial Search Technology within the UK Police National Database (PND)**

11. In March 2014, the Home Office introduced a UK wide facial searching functionality within PND to enable the police to search facial images of potential suspects against police records. The system provides a 'facial search' rather than a facial recognition capability as any potential matches returned by the system require human assessment to ascertain whether the returned images may be a match for a potential suspect. In essence though, this created a searchable database of UK police records, including the ability to automatically search images of people who were not necessarily yet convicted. It also introduced the ability of searching third-party sourced images of suspects (known as probe images) against that database such as CCTV records obtained by the police, or images taken by the public on mobile telephones and

---

<sup>9</sup> [The Bichard Inquiry, Report](#).

<sup>10</sup> Bichard Inquiry report 2004, paragraph 4.17, page 130.

<sup>11</sup> *Ibid*, paragraph 4.29, page 131.

<sup>12</sup> The Metropolitan Police do not upload custody images to PND as a result of a 2012 legal ruling in the High Court of Justice. The case involved the retention of data on PND about a juvenile who had not subsequently been convicted of the offence to which the data related. The court concluded that the retention of the claimant's photographs in application of the existing policy amounted to an unjustified interference with their right to respect for their private life and was a breach of Article 8 of the European Convention on Human Rights. See [RMC and FJ v Metropolitan Police Commissioner Judgement](#) 2012.

subsequently handed to the police as part of an investigation, or from police body-worn video (BWV) cameras.

12. In February 2015 (and as he had done in his 2014 Annual Report) the Biometrics Commissioner for England and Wales Alastair MacGregor QC raised concerns on the BBC Newsnight Programme about the lack of an appropriate regulatory regime around the uploading of custody photographs to the PND and the use of facial searching technologies by the police in England and Wales. It was also widely reported by the popular media that some forces in England and Wales had uploaded images of people who had not been charged with any crime or offence. In June 2015, there was further media interest when it was reported that 90,000 people attending a music festival in Derby would be biometrically scanned by Leicestershire Police to compare their facial images with those held on local police records.<sup>13</sup> This was inaccurate media reporting as Leicestershire Police were not using PND Facial Search at this event and PND does not have the capability to be deployed in this manner.
13. Police Scotland has been using the facial searching functionality within PND since 2014 to identify suspected criminals and Police Scotland had previously advised Scottish Ministers that as at 27 May 2015, it had used PND 494 times for facial recognition searches.<sup>14</sup> As at 22 April 2015, there were 601,837 Scottish images of 334,594 people with CHS records on PND. At this time there were 11.8 million images in PND meaning that Scottish CHS records accounted for 7.1% of the total.

### Key Research Questions

14. Against this introductory context, this HMICS Audit and Assurance review sought to answer the following eight key research questions:
  - What is the statutory framework that underpins the police use of images and facial search technologies in Scotland?
  - What is the current policy and practice adopted by Police Scotland and what Standard Operating Procedures (SOPs) or written guidance exists in relation to the use of the facial search functionality within PND?
  - How many of the 494 uses of the PND facial search technology comply with Police Scotland's written policy and legislation?
  - What Police Scotland governance and oversight arrangements are in place around facial searches on PND, how are ethical issues considered, and is there a clear audit trail of all facial search applications and authorisation decisions including any which may have been refused?
  - What are the administrative and technical interfaces between the Police Scotland Criminal History System (CHS) and the wider UK Police Database (PND)?
  - What governance and assurance arrangements are in place around recording, weeding and retention of information and records on CHS, and is this applied consistently across Scotland?
  - What are the comparisons with the police operational use of facial search technologies in England and Wales and what are the wider opportunities and threats from the police use of such new and emerging technologies?

---

<sup>13</sup> ITV report, [Download Festival: Police use facial recognition technology on revellers](#), 13 June 2015.

<sup>14</sup> Police Scotland response to questions raised in Scottish Parliament in May 2015.

- How does Police Scotland interface with wider UK governance arrangements around PND, and how do the arrangements in Scotland align with current Home Office PND Codes of Practice for England and Wales?

### Methodology

15. Our methodological approach sought to answer the key research questions and comprised of a blend of qualitative and quantitative research techniques to fully explore the use by Police Scotland of the facial search capability within the PND. We achieved this by using our Inspection Framework and by examining Police Scotland practice against professional and technical guidance.

As part of this we conducted:

- An audit of 567 records of Police Scotland's use of the facial search technology within PND. Sample included all instances of use by Police Scotland from 28 March 2014 to 8 July 2015.
- A review of Police Scotland's written policies and procedures relative to CHS, PND and the use of facial search technology capabilities within PND. This included reviewing Police Scotland procedures against wider Home Office and College of Policing technical guidance manuals on the use of PND search.
- An examination of case study evidence pointing to the success or otherwise of the use of facial search technologies by Police Scotland.
- A review of the statutory framework that underpins the police use of facial images and other biometric data samples in Scotland.
- Interviews with a small number of senior officers and senior staff with key governance and assurance responsibilities for CHS, PND and Records Management within Police Scotland.
- Benchmarking with a limited selection of forces in England and Wales.
- Interviews with a small number of other stakeholders as necessary to achieve the aims of our audit and assurance review.

# The statutory framework for the police use of images and biometric samples in Scotland

---

## Historical Context

16. The use of photographic images and other biometric technologies are not new developments in policing and therefore before examining the statutory framework for the police use of images and other biometric samples in Scotland, it is useful to firstly reflect upon the historical and international context within which such technologies have evolved.

## Police photographic images

17. The police have taken photographic images of people arrested and charged with crimes and offences in Scotland for more than 100 years.<sup>15</sup> In the wider UK, the police in Liverpool and Birmingham are known to have been photographing criminals since 1848.<sup>16</sup>

18. In 1888, Alphonse Bertillion (1853-1914) invented the modern method of photographing people who have been arrested and charged by the police. His approach centred on full face and profile views of the prisoner with a standardised distance between the camera and the subject and standardised lighting and angles. This system is now widely referred to as a police 'mug-shot' and it had been universally adopted throughout the international policing and law enforcement community by the late nineteenth century.

19. Bertillion was a French police officer and biometrics researcher based in Paris who applied the anthropological science of anthropometry<sup>17</sup> to law enforcement creating an identification system based on physical measurements of facial characteristics. Anthropometry was the first scientific system used by the police to identify criminals. Before that time, criminals could only be identified by name or witness testimony.

20. In 1960, the first unified Scottish Criminal Records Office (SCRO) was established in Glasgow and the Police (Scotland) Act 1967 subsequently provided a statutory framework for the retention of criminal records and fingerprints until more comprehensive guidance was provided in the Criminal Procedure (Scotland) Act 1995. These national arrangements were in place under legacy policing structures over 50 years prior to the creation of Police Scotland.

## Police use of Fingerprints

21. The police in the UK have also been taking and using fingerprints as a means of biometric identification for more than 100 years. In 1880, Dr Henry Faulds, a Scottish physician, wrote an article in the journal 'Nature' suggesting that fingerprints would be useful as a technique for investigation of evidence left at the scene of a crime. In 1900, the UK Home Secretary conducted an inquiry into 'Identification of Criminals by Measurement and Fingerprints' and subsequently the adoption of fingerprinting was formally introduced in 1901 when the Metropolitan Police created the first UK Fingerprint Branch at New Scotland Yard in London.

---

<sup>15</sup> Source, HMICS archives and annual reports dating from 1865, St Andrew's House, Edinburgh.

<sup>16</sup> Norfolk, L. (2006) 'A history of twentieth Century Mugshots' published in The Telegraph (London). 17 September 2006.

<sup>17</sup> Anthropometry (from Greek *ἄνθρωπος* *anthropos*, "man" and *μέτρον* *metron*, "measure") refers to the measurement of the human individual.



## Police use of DNA technologies

22. In Forensic Science the process of analysing DNA is referred to as DNA profiling, and in Scotland, this involves targeting 24 specific parts within the DNA known as Short Tandem Repeats. This technology makes it possible to compare a DNA profile from a person, known as a reference sample, with a DNA profile from an evidence crime sample. If there is a match between the DNA profile from the person and that of the crime sample then the probability of finding this match if the DNA did not come from that person is 1 in more than 1 billion. This is why DNA has become so important in criminal investigations as it can be used to provide evidence of the presence or contact by the suspect.
23. DNA was first used in criminal analysis in the UK in the 1980s following a double rape and murder in Leicestershire. This led to the production of the first DNA profile which showed that both murders had been carried out by the same individual, who was not the prime suspect.

## Statutory Framework for Criminal Justice Samples in Scotland

24. The Criminal Procedure (Scotland) Act 1995 is the primary Scottish legislation allowing the retention of prints and other biometric samples from a person arrested or detained by the police.<sup>18</sup> Sections 18, 19 and 20 stipulate the conditions under which samples may be taken by the police, and the limitations and conditions to which they may be put.
25. Section 18 (2) states: 'A Constable may take from the person, or require the person to provide him with, such relevant physical data as the Constable may, having regard to the circumstances of the suspected offence in respect of which the person has been arrested or detained, reasonably consider it appropriate to take from him or require him to provide, and the person so required shall comply with that requirement'
26. The Criminal Procedure (Scotland) Act 1995 does not explicitly reference facial images and defines 'relevant physical data' as 'a fingerprint, palm print, print or impression of an external part of the body or record of a person's skin on an external part of the body created by a device approved by the Secretary of State'. However, the term biometric data is usually thought to include facial images and voice patterns.<sup>19</sup>
27. Section 83 of the Police Public Order and Criminal Justice (Scotland) Act 2006 inserted an additional Section 18A into the Criminal Procedure (Scotland) Act 1995 which contains provisions to retain DNA Samples and Profiles of persons who have been arrested but not convicted of certain sexual or violent crimes. The list of relevant sexual and violent offences is defined in Section 48 of the Crime and Punishment (Scotland) Act 1997.
28. In 2010, the Scottish Government introduced the Criminal Justice and Licensing (Scotland) Act, 2010 which included a number of provisions to enhance public protection and improve the law in relation to the retention and use of DNA, fingerprints and other physical data. Full details can be found in Sections 77 to 82 of the Act.

---

<sup>18</sup> In Scotland, the police do not routinely take biometric samples for all types of crimes or offences. It is only used for persons arrested or detained and brought to a police station in connection with specified common law crimes or specified statutory offences.

<sup>19</sup> Biometrics Commissioner: *Oral Evidence to House of Commons Science and Technology Committee on current and future uses of biometric technologies*, 10 December 2014.

29. In brief terms, the statutory framework in Scotland for the retention of fingerprints and DNA biometrics is as follows:
- Fingerprints, and DNA data from convicted individuals is retained indefinitely;
  - Data from individuals prosecuted for certain sexual and violent offences may be retained for three years (whether or not they are convicted), with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of any particular person's data); and
  - Data from individuals arrested for any offences must be destroyed immediately if they are not convicted or if they are granted an absolute discharge.
30. Whilst it has been custom and practice for the police to take photographic images of persons who have been arrested or detained for more than 100 years in Scotland, there is no specific legislation which gives statutory powers to the police to take such images.<sup>20</sup> There is also no qualifying legislation which subsequently governs or regulates the retention periods for such images or indeed the way in which such images may be used.<sup>21</sup> This means the Scottish legislation around biometric retention by the police centres primarily on fingerprints and DNA data and not on data pertaining to photographic images.
31. Clearly, when retaining fingerprints and DNA within the parameters of the current legal framework in Scotland it is essential for the police to also retain the corresponding photographic images to which those fingerprints and DNA samples relate. However, on non-conviction, Police Scotland has one set of weeding and retention policies for photographic images held on CHS which largely mirror the destruction arrangements for fingerprints and DNA, and a different set of weeding and retention policies for images held on police custody systems. This means that CHS images of people are generally destroyed on non-conviction, whilst the same images pertaining to the corresponding custody episode are retained for a period of at least six years<sup>22</sup>. In the case of custody images, this includes the retention of images of people who have been arrested or detained but who have not been charged or convicted with any offence.
32. This retention policy is based on that which was formerly adopted by ACPOS under legacy policing arrangements in Scotland, but we are aware that Police Scotland is currently reviewing its data retention policies. As mentioned earlier in this report, the reason that custody images are retained is to assist in the investigation of circumstances where arrested persons may have provided false identity details to the police or other circumstances such as retrospective complaints being made about a particular custody episode.
33. Therefore in the absence of specific legislation, the statutory framework for retention in Scotland of fingerprints and DNA is voluntarily applied to photographic images on CHS and PND. Whilst Police Scotland only uploads custody images to CHS and PND as a pending case as a result of a person having been charged with a crime or offence, it does also retain all images in its custody software for periods of at least six years. This

---

<sup>20</sup> Schedule 2, paragraph 1 (j) of the Police and Fire Reform (Scotland) Act does state that a police custody and security officer has the power to take photographs under the direction of a constable but there is no primary legislation giving a constable the power to take such images.

<sup>21</sup> In relation to custody images, Police Scotland cites both the Prescription and Limitation (Scotland) Act 1984 and the Public Records (Scotland) Act 2011 with regard to having stated retention standards. Neither of these sources contains any specific legal references relating to the retention or use of police photographic images.

<sup>22</sup> Images will be retained on non-conviction to update criminal records in circumstances where the accused person already has an established criminal record.

position has some resonance with the approach to custody images in England and Wales where the Biometrics Commissioner has made it clear that the legislation applying to fingerprint and DNA retention does not apply to photographic images.

34. While we are satisfied that Police Scotland is retaining photographic images on both CHS and PND in an appropriate manner, we believe there is an opportunity to close a potential legislative gap in Scotland. This would provide greater clarity around the retention of all types of photographic images held by the police for differing reasons and also greater clarity on the purposes for which such images may be used. Such legislation would balance the needs of law enforcement with broader human rights and ethical considerations, and would also provide a statutory framework which balances the needs of policing with the wider societal opportunities and threats that arise from the police use of new and emerging technologies.
35. We would therefore encourage Scottish Government to work with Police Scotland and the Scottish Police Authority to consider additional legislative provisions to enhance public protection and improve and clarify the law in relation to the retention and use of photographic images by the police.

### Recommendation 1

Scottish Government should work with Police Scotland and the Scottish Police Authority to consider legislative provision in relation to the retention and use of photographic images by the police.

36. More broadly, it should be noted that The European Court of Human Rights has previously drawn specific positive attention to the Scottish statutory framework around biometrics in its judgment in *S and Marper*:<sup>23</sup>

*[109]. The current position of Scotland, as a part of the United Kingdom itself, is of particular significance in this regard. As noted above..., the Scottish Parliament voted to allow the retention of DNA of unconvicted persons only in the case of adults charged with violent or sexual offences and even then, for three years only, with the possibility of extension to keep the DNA sample and data for a further two years with the consent of a sheriff.*

*[110]. This position is notably consistent with Committee of Ministers' Recommendation R(92) 1, which stresses the need for an approach which discriminates between different kinds of cases and for the application of strictly defined storage periods for data, even in more serious cases. Against this background, England, Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence.*

37. In connection with the police use of other biometric samples, it should also be noted that Section 82 of the Criminal Justice and Licensing (Scotland) Act, 2010 amended the Criminal Procedure (Scotland) Act 1995 to permit the use of samples for the purposes of the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution. All references to crime, investigation and prosecution in the primary Scottish legislation include provisions for the use of such samples for those same purposes in other parts of the UK, or in a country or territory outside Scotland.

---

<sup>23</sup> Case of *S. And Marper v The United Kingdom*, Applications nos. 30562/04 and 30566/04, paragraphs 36 and 109-110.

These statutory provisions are contained within Section 19 (c) of the Criminal Procedure (Scotland) Act 1995. Reciprocal arrangements exist within legislation applicable to England and Wales through the Criminal Procedure and Investigations Act 1996, and with other jurisdictions.

38. However, there are important legislative differences across the UK in relation to the rules which may be applied in connection with the retention of fingerprints, DNA and other criminal justice samples with stricter conditions applying under Scottish law. In response to the European Court of Human Rights concerns, The Protection of Freedom Act introduced a new biometrics regime in England and Wales in 2012. We will discuss comparisons with England and Wales later in this report but it is important to point out that differing arrangements for images across the UK are being applied to the common UK PND database. This means that the PND gives Police Scotland access to information from England, Wales and Northern Ireland from biometric records arising from circumstances where the retention of such information would not have been permissible under current policy had the record been created in Scotland.
39. As mentioned earlier in this report, the PND is a confidential and restricted intelligence system and therefore although Police Scotland can legally access photographic image data from custody episodes in England, Wales and Northern Ireland any output serves purely as an intelligence product and cannot be used for evidential purposes. It does however highlight a potential ethical dilemma which we discuss further in paragraphs 89 and 90 of this report leading to a recommendation around the potential development of a statutory code of practice for the use of biometric data in Scotland<sup>24</sup>.
40. A basic process map showing the biometric sample journey within the wider Criminal Justice Process in Scotland is included as **Appendix 1** to this report. The process map is included to help readers visualise the sample journey and standard key decision points. However readers should also be mindful of the additional retention provisions for violent and sexual offenders as outlined above.

### **Governance arrangements for police use of biometrics in Scotland**

41. Before turning to consider the current governance arrangements around the police use of biometrics it is useful to reflect on what has already been said about police biometric governance in Scotland. It is also useful to note that the terms forensics and biometrics are sometimes used interchangeably.

### **The Fraser Report**

42. In 2007 the Scottish Government asked forensics expert Professor James Fraser to review the operation and effectiveness of the legislative regime governing police powers in relation to the acquisition, use and destruction of fingerprint and DNA data. He was directed to consider additional powers in so far as they relate to the retention of forensic data.
43. In 2008 his report was published and made eight recommendations, many of which formed provisions within the Criminal Justice and Licensing (Scotland) Act 2010.<sup>25</sup> Two recommendations which were not taken forward into statute were:

- a) ***The current governance arrangements for DNA and Fingerprint databases in Scotland should be reviewed as a matter of urgency. Future arrangements should take into account good practice in scientific and ethical standards, efficient and effective management and independent oversight.***

<sup>24</sup> See paragraph 89 and Recommendation No 4 of this report.

<sup>25</sup> Fraser Report, 2008.


- b) Sufficient information regarding the governance and management of forensic databases should be in the public domain to maintain transparency, accountability and public confidence in their use.***

#### **Existing Biometric Governance Arrangements**

44. The recommendations from the Fraser Report related solely to the Scottish fingerprints placed on IDENT1 and the Scottish DNA Database (SDNAD) both of which are maintained by the Scottish Police Authority. However, both of these databases actually sit on ICT platforms located within Police Scotland operational environments and therefore any concerns or appeals from members of the public are firstly directed to Police Scotland, where the ACC Major Crime and Public Protection considers the matter with the assistance of Police Scotland staff from National Systems Support.
45. By contrast, the CHS is entirely maintained by Police Scotland. The specific Police Scotland governance arrangements for CHS and PND will be described later in this report, however when considering broader debates around biometrics it is useful to touch briefly on the related governance arrangements for fingerprints and DNA.
46. Collection, management, extraction and storage of DNA cuts across many policing divisions: the responsibility for the collection of samples lies between Local Policing and Custody Division; the management of records on the SDNAD and compliance with relevant legislation rests with Police Scotland's National Systems Support; profiling, storage and searching resides with SPA Forensic Services; and Specialist Crime Division (SCD) being the recipient of crime scene match reports. The strategic oversight of DNA and the SDNAD within Police Scotland is provided through Specialist Crime Division (SCD) with the Assistant Chief Constable Major Crime and Public Protection being the Information Asset Owner.

#### **Scottish DNA Database (SDNAD) and UK Fingerprint Database (IDENT1)**

47. The Scottish DNA Database was established following the introduction of the Criminal Procedure (Scotland) Act 1995, which legislated for forensic data to be provided from arrested or detained persons. Profiles from the SDNAD are also exported to the UK DNA Database (NDNAD). Scottish fingerprints by contrast are held on IDENT1 which is the single, searchable database for the UK mainland for finger and palm print data. Instead of searching crime scene marks against a Scottish database of 360,000 prints, the Scottish Police Authority (SPA) can search against a UK database of 6.5 million prints, providing the potential for more identification.
48. The SPA manages SDNAD and Scottish records interface to IDENT1 and works in partnership with Police Scotland, SPA Forensic Services and COPFS. To improve the governance processes around how the SPA delivers forensic services to Police Scotland, a Forensic Services Strategic Partnership Forum was established and similar groups operate at tactical and operational levels. These forums provide internal governance around how forensic services are delivered to Police Scotland but they do not provide independent or external oversight over the use of biometric data for policing purposes.
49. Whilst it is clear from our review that effective internal governance arrangements exist between key partners, those arrangements clearly do not amount to the independent oversight of the management of DNA or fingerprints in Scotland as called for in the Fraser Report. This contrasts with the position in England and Wales where the Protection of Freedoms Act, 2012 led to the introduction of a new biometrics regime including the appointment of an independent Biometrics Commissioner. The Biometrics Commissioner has jurisdiction over England and Wales only, but also has a broader UK role on reserved matters of UK National security.

- 
50. The SPA, Police Scotland and COPFS have recognised through discussions at the Forensic Services Strategic Partnership Forum that there is still work to be done in Scotland to address the issues of ethical and independent oversight. At the time of our audit and assurance review we were able to review developing Police Scotland and SPA policy papers calling for the establishment of an independent ethics group to provide advice, assistance and opinion on DNA data and sample management within the Scottish context. Whilst we welcome this potential development, we do not believe that the envisaged remit of providing advice, assistance and opinion is sufficient to fully discharge the call made in the Fraser report for completely independent oversight and it would also fall short of the arrangements now established in England and Wales.
  51. During the course of our review we met with the Biometrics Commissioner for England and Wales and gained a valuable insight into his role. Whilst we welcome ongoing policy development in this area in Scotland, we also believe that consideration should now be given by Scottish Government to the creation of a Scottish Commissioner so that public confidence in the police use of biometrics can be maintained through an independent office. This could assist in the delivery of truly independent oversight of the police use of biometrics including DNA, fingerprints and photographic images. Through the production of an annual report to the Scottish Parliament, it would also assist in providing more robust transparency and accountability to the people of Scotland on the use of biometric data for policing purposes.
  52. Such a post could also build capacity and resilience within Scotland to explore emerging human rights and ethical considerations around the use of biometric data by other public agencies including matters which have recently been at the fore of public debate such as biometric data held on public space CCTV systems, Road Camera Enforcement Systems which capture facial images, and also Automatic Number Plate Recognition Systems (ANPR) in use on average speed camera systems which can also capture facial images of drivers.<sup>26</sup> Clearly new and emerging technologies escalate the value and possibilities around the use of biometric data and when combined with the development of underpinning codes of practice, our view is that the creation of an independent Scottish Commissioner could both safeguard and future-proof what will undoubtedly continue to be a fast and evolving scientific landscape. We acknowledge that whilst this could be achieved through the creation of a new commissioner, there may equally be scope to align these responsibilities within existing or rationalised structures.

## **Recommendation 2**

Scottish Government should work with Police Scotland, the SPA, COPFS and other interested parties to consider the establishment of an independent Scottish Commissioner to address the issues of ethical and independent oversight of biometrics records and databases held in Scotland, with sufficient flexibility to embrace future technologies and relevant codes of practice.

---

<sup>26</sup> We discuss surveillance cameras later in this report under the chapter on comparisons with England and Wales including the CCTV Surveillance Camera Commissioner for England and Wales introduced under the Protection of Freedoms Act 2012.

# Police Scotland policy and practice in relation to the Criminal History System (CHS) and the UK Police Database (PND)

---

## CHS policy

53. During the course of our audit and assurance review, we reviewed the Police Scotland Standard Operating Procedures (SOP) for CHS.<sup>27</sup> From examination of this restricted document we noted that it contained comprehensive guidance for officers and staff on the operation of the various functions and capabilities within CHS, and of the legal and other regulatory frameworks within which the system can be used. From our independent analysis of those procedural arrangements, we are satisfied that the arrangements described therein are fully compliant with current legislation including the Data Protection Act 1998 and the Human Rights Act 1998. They also comply with the Authorised Professional Practice (APP) contained in the College of Policing Management of Police Information (MOPI) Guidance, albeit that legislatively MOPI does not apply to Scotland.<sup>28</sup>
54. As noted, MOPI, which governs PND is not applicable to Scotland. However, Scotland did adopt the principles in 2007; not least because they were already being met through the prevailing ACPOS Information Management procedures in place at the time. The Home Office are currently reviewing MOPI with focus on the retention of records to ensure the appropriate and current management of records. Scotland's current retention management processes are seen as best practice by the Home Office.
55. Although Police Scotland has a single CHS, local administrative arrangements exist within local police records management units across Scotland that largely mirror legacy force criminal justice administration arrangements with key local partners. These arrangements are fully described in the Police Scotland CHS SOP and largely centre on the local arrangements for systems access, staff training and system updates and requests. Police Scotland has also published its weeding and retention policies for CHS on the Police Scotland website.<sup>29</sup> As mentioned earlier in this report, Police Scotland is currently reviewing its data retention policies as part of a broader programme of work to introduce the new i6 suite of ICT systems including a single custody system for Scotland.
56. From our audit and assurance review activities, we can confirm that Police Scotland policy around CHS is consistently applied throughout Scotland. We describe these arrangements in more detail when we explore the administrative and technical interfaces between CHS and PND later in this report.

## PND policy

57. As part of our audit and assurance review we also examined the Police Scotland SOP for PND.<sup>30</sup> The SOP provides comprehensive guidance to officers and staff on how PND is to be used by Police Scotland and contains details of the system of governance. The SOP makes it clear that PND is a confidential intelligence handling


---

<sup>27</sup> Version 1.01 published 22 July 2013: GPMS Restricted.

<sup>28</sup> College of Policing (2014): *Management of police information* [Internet]. <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/> [Accessed 23 July 2015].

<sup>29</sup> Police Scotland, *Recording, Weeding and Retention of Information on Criminal History System (CHS)*, August 2013.

<sup>30</sup> Versions 1.0 dated 22 July 2013 and 2.0 dated 01 July 2015: GPMS Restricted.



system and not an evidential system. The Police Scotland SOP addresses ethical considerations such as the procedure to be followed when handling data that does not belong to Police Scotland. Having independently reviewed the procedural arrangements described in the Police Scotland policy on PND, we are satisfied that the arrangements described therein are fully compliant with existing legislation including the Data Protection Act 1998 and the Human Rights Act 1998.

58. Police Scotland does not have a stand-alone SOP for the use of the facial search functionality within PND as specific guidance is available to PND operators through relevant confidential or restricted UK police guidance manuals including the Home Office: PND Facial Searches Guidance 2014 and the College of Policing: PND Search User Guidance: 2015. However, the Police Scotland SOP does contain brief information on the facial search capability within PND and provides references to the Home Office and College of Policing guidance.
59. We reviewed the content of the Home Office: PND Facial Searches Guidance 2014 and the College of Policing: PND Search User Guidance 2015 and used these confidential information sources to assess how well Police Scotland were complying with UK police guidance when we examined every instance of the use of the facial search capability within PND conducted by Police Scotland up to and including 8 July 2015. The results of our audit can be found in the following section of this report.



# Findings from our audit and review of use of the facial search functionality within PND by Police Scotland

---

60. A key research question for our audit and assurance review was to ascertain how many times Police Scotland had made use of the facial search capability within PND and how many of those uses were compliant with Police Scotland written policy and other guidance and legislation.
61. To determine this, we firstly reviewed the relevant Police Scotland PND SOP and we also reviewed the restricted UK police guidance materials on the use of PND produced by the Home Office and College of Policing, as previously described. Before turning to the results of our audit, it is useful to briefly explain how the facial search works within PND, and also to reflect on what policing purposes facial search may be used for.


## How Facial Search within PND Works

62. In general terms, the PND Facial Search facility enables authorised users to upload an image into the PND and search across all person images attached to person records or custody records (England and Wales) to see if there are any suggested matched images. The image being uploaded is known as the probe image, and in essence, what PND does is compare that image against all other images held in the system. This takes place in an area of the system known as the gallery, and so for the purposes of this report we will refer to these as gallery images. Importantly, probe images are not retained on the PND system after a search has been conducted.
63. The UK PND guidance makes it clear that other policing systems such as the UK Police National Computer (PNC) must firstly be checked when trying to ascertain the identity of a specific subject before making use of any of the various search capabilities within systems such as PND.<sup>31</sup> However, Facial Search can be of particular value when the police are dealing with fraudulently obtained documents such as fraudulent passports or photographic driving licences as often the only genuine detail on such documents is the facial image. Importantly, the technology can also be used to eliminate suspects from enquiries and establish innocence as well as pointing to the potential identity of an accused.
64. The Facial Search actually works by pinpointing key biometric points on the face (such as the eyes, ears, nose and chin) and allocating them a numerical value. Each probe image can then be searched against all gallery images within the PND to identify any images with a similar numerical value. This enables the PND to bring back images of individuals irrespective of whether they have aged, started wearing glasses, changed hair-style and/or gained/lost weight.<sup>32</sup>

---

<sup>31</sup> The Police National Computer (PNC) is the primary national police computer system in the United Kingdom and is used for facilitating investigations and sharing information of both national and local significance. The system provides intelligence to police and other criminal justice or law enforcement agencies by holding extensive information on people, vehicles, crimes and property. It is accessible over a secure network, within seconds and from thousands of terminals across the country at any time. This now includes mobile data checking at the scene of a crime or investigation. The Scottish Criminal History System (CHS) feeds and weeds Scottish data into PNC and PND.

<sup>32</sup> In order for a probe image to be analysed, it must be 500kb or less and the number of pixels between the subjects pupil must be at least ten percent of the total width of the picture.


- 
65. These search capabilities within PND are a useful policing tool but do not amount to true facial recognition. Instead it offers a technological solution intended to make existing and long-standing manual search processes more effective and efficient.
  66. During the course of our review, we were given a demonstration of the system by Police Scotland so that we could understand more fully how the system works in practice. After upload of a probe image, the system returned a list of up to 50 potential matches ranked by PND from most likely to least likely. Human assessment was then required to narrow the search further, for example eliminating returned images of persons of the opposite sex. As the search parameters are refined by the PND operator, it will often be necessary for a fresh search to be initiated of the same probe image meaning that many probe images are searched more than once.
  67. In many cases, the system will actually be unable to point to the potential identity of the subject. In the event of a potential match, the information is passed as an intelligence product to the relevant enquiry officer for further development of the intelligence. The PND system is therefore unable to say how many successful identifications have been made as it simply produces an intelligence output for further consideration and investigation by traditional human means. It is however understood that the Home Office are to commission a business benefits analysis of the effectiveness of PND, and Police Scotland plan to do likewise once the final stage of PND delivery in Scotland relating to the Scottish Intelligence Database (SID) is completed in 2016.

#### **Searching on PND and PND Search Reason Codes**

68. Home Office and College of Policing guidance provides that PND must only be used to research a “lawful, necessary, proportionate, relevant and realistic task”. All tasks should have a justification which may include a local reference number to link the PND search to the wider business process. The PND is to be used solely for policing purposes. This is defined in the guidance as:
  - Protecting life and property
  - Preserving order
  - Preventing the commission of offences
  - Bringing offenders to justice
  - Any duty or responsibility of the police arising from common or statute law
69. The use of the PND and any data obtained from it must comply with the principles of the Human Rights Act 1998 and be:
  - Lawful
  - Proportionate
  - Necessary
70. When conducting a search on PND, the PND Operator must complete a number of mandatory search codes. This includes categorising the search into one of nine PND search reason codes.

#### **The results of our Audit**

71. As part of our audit and assurance review we asked Police Scotland to provide us with access to an extract of data relating to all uses of the Facial Search capability within PND from its introduction in March 2014 to the date that our fieldwork commenced on



8 July 2015. This confidential data was extracted from PND by a Home Office PND Auditor into a spreadsheet with data fields to our requested specification. This included fields which cross referenced to the unique relevant crime or incident report identification numbers and details of the requesting officer and relevant authorisation.

72. This produced a return of 567 individual searches conducted by Police Scotland over a 16 month period. The 567 searches related to 330 probe images (330 images of people) meaning that many probe images had been searched more than once.
73. Having reviewed the confidential detail of each and every one of these instances of use of the PND facial search capability, we found 100% compliance with Police Scotland policy and with Home Office and College of Policing Guidance. Accordingly, we conclude that all uses by Police Scotland have been lawful, proportionate and necessary. The searching of 330 probe images by Police Scotland over a 65 week period also means that on average Police Scotland have searched around 5 probe images per week which is less than 1 search per day being conducted in Scotland.
74. The results of our audit are summarised by the following table which shows the number of searches conducted by Police Scotland by the nine PND Search Reason Codes. Categories 1 to 3 relate to public protection, the vetting category included issues such as firearms or explosives applications and intelligence development is a broad category encompassing high volume crimes such as theft and fraud that fall within the defined policing purposes as specified in Home Office Guidance. This was the most commonly used reason code and in our key facts pie chart we refer to these various crime types as 'volume crime' for ease of reference. There were no examples whatsoever of Police Scotland using the PND facial search in connection with sporting or other public events and all uses related to the investigation of specific individual crimes or incidents or legitimate policing enquiries.<sup>33</sup> This table is also presented as pie charts in the key facts section earlier in this report.

---

<sup>33</sup> 17 searches were test searched by newly trained operators and did not therefore relate to a specific crime or incident.

<b>PND Search Reason Codes<sup>34</sup></b>	<b>Number of individual searches by Police Scotland by PND search reason code<sup>35</sup></b>	<b>Number of images (different people) these searches related to<sup>36</sup></b>
Child abuse	15	10
Domestic abuse	0	0
Vulnerable adult	1	1
Police vetting	6	4
Counter terrorism	3	3
Intelligence development (Volume Crime)	405	235
Economic crime	21	12
Serious crime	99	49
Other <sup>37</sup>	17	16
<b>Totals</b>	<b>567</b>	<b>330</b>
Number of PND searches by Police Scotland found to comply with Home Office and College of Policing Guidance and Police Scotland Standard Operating Procedures.	<b>567 (100%)</b>	

Table No 1: Facial Searches conducted by Police Scotland by PND reason code from 01 March 2014 to 08 July 2015.

75. In terms of administrative arrangements, Police Scotland has an internal PND Request Form (Form md2) which operational officers can complete to request a PND search. This form relates to all types of PND search and not just facial search. The guidance on the form states that a PND search may be authorised for the purposes of public protection, counter-terrorism, major crime and serious and organised crime. Should the request come from a front-line officer, it requires to be authorised in the first instance by their line manager who then e-mails the authorisation to the appropriate PND operator. Applications which are not approved are not centrally collated and therefore we were unable to establish from Police Scotland how many facial search applications had been refused.
76. Alternatively, application for a PND search can be e-mailed without the request form to the appropriate PND operator explaining the policing purpose for the request in which case the search can be authorised by the PND operator providing that the request relates to a legitimate policing purpose as specified in the College of Policing PND Search User Guidance Manual. In the case of a PND operator who works in an intelligence development role, he/she is not required to submit such applications as this forms a core part of their duties and is recorded on PND in any event.
77. During our audit and assurance review we learned of some minor regional variations in approach and we also noted that these four broad search reason headings in the request form do not align directly with the nine distinct Search Reason Codes on the PND system. We also note that the PND Search Reason Codes are to be updated in March 2016. Whilst we are satisfied that all uses of the facial search functionality on

<sup>34</sup> Facial image searches carried out on PND by Police Scotland between 01 March 2014 and 08 July 2015.

<sup>35</sup> These are the authorised search reason codes contained within the Home Office, PND Facial Searching Guidance Manual: 2014 (GPMS Official / Sensitive) and the College of Policing, PND Search User Guidance Manual: 2015 (GPMS Official/Sensitive).

<sup>36</sup> Some images of the same person will be searched more than once as part of the narrowing down process by a PND operator during the course of a search which may initially return one hundred or more images which may potentially be similar to the subject being searched.

<sup>37</sup> All 17 searches in this category were found to be test searches by newly trained operators.

PND have been entirely appropriate, we recommend that Police Scotland should amend the PND Request Form so that permissible search criteria are more clearly understood by operational staff, and so the requests and authorisations can be categorised at the outset to align directly with the appropriate PND Search Reason Code. In relation to variations in regional approach and absence of a central register of applications, we are satisfied that all approved requests can be audited on the live system and that Police Scotland had arrangements in hand at the point of our inspection to standardise the application process for requested searches of PND.

### **Recommendation 3**

Police Scotland should amend its internal PND Search Request Form so that the reasons for requested PND searches are coded to align directly with the PND Search Reason Codes in the live database.

### **Sanitised Case Studies from our review**

78. Although our audit of the use of facial search shows that Police Scotland are making very limited and selective use of this PND functionality, it may be useful for readers to understand the types of crimes and incidents where its application can add real value. Accordingly, we provide the following two sanitised examples which were obtained from PND users as part of our broader assurance activity:

#### **Case Study Number 1**

A female living in Scotland was being persistently stalked by an unknown male. On one instance she was able to take a 'side-on' photograph of the male on her smart phone and she made the image available to the police. The probe image was uploaded to PND but initially no potential matches were found. The PND operator repeated the search some nine days later using a better digital image and this time the system returned a potential match. A male with a history of sex offending was subsequently identified and charged. This example illustrates the value of the same probe image being searched more than once against gallery images on PND.

#### **Case Study Number 2**

Police Scotland obtained an image from CCTV in a bookmakers shop whilst investigating a serious assault. The image showed the male suspect who had followed another man from the bookmakers to a nearby street where he violently assaulted him and bit off part of his ear before stealing his mobile phone. There was no evidence as to the identity of the assailant other than the CCTV image. The probe image was uploaded to PND and the facial search returned information which subsequently led to the male being identified, arrested and charged.

79. These two sanitised examples relate to the identification of offenders in Scotland by Police Scotland. However, as PND is a UK policing system this also means that facial search offers the potential to assist in the identification of travelling criminals and members of serious and organised crime groups who operate throughout the UK. The following sanitised example from Durham Constabulary shows how a travelling criminal from England previously arrested by Police Scotland was identified for crimes in England as a result of the CHS image uploaded to PND by Police Scotland.



### Case Study Number 3

A theft occurred at a bookmakers shop in Durham where money was stolen from the till. The shop CCTV showed a man leaning over the counter and he was presumed to be the suspect. Durham Constabulary conducted a facial search of the probe image on PND which suggested a possible lead. Further enquiries showed that this person had been arrested by Devon and Cornwall Police the week previously, and was also known to Surrey Police. The gallery image within the main PND database which identified the potential match had been uploaded from the Police Scotland CHS system some months earlier after the subject had been arrested in Scotland. An arrest package was sent to Surrey Police and the suspect was arrested and admitted the Durham offence. He subsequently pled guilty in court.

80. Collectively, these three sanitised case studies demonstrate how the facial search functionality within PND can sometimes produce an intelligence product which can then be passed to an investigating officer for further investigation by conventional means. We have highlighted earlier in this report that PND gives Police Scotland access to images from England and Wales arising from circumstances where such an image would not have been retained under current policy had the record been created in Scotland and the potential ethical dilemma that this presents. However, during our audit and assurance review we did not find any actual examples of a suspect in Scotland having been identified from custody images of a non-convicted person from England and Wales. Should this scenario arise, we are satisfied that Police Scotland has detailed guidance in its PND Standard Operating Procedures and it is worth reiterating that images held on PND are not used for evidential purposes.

## Governance arrangements for PND

---

### UK Policing governance arrangements for PND

81. The PND Partners for policing in the UK includes all 43 forces in England and Wales, Police Scotland, the Police Service of Northern Ireland, British Transport Police, National Crime Agency, Civil Nuclear Constabulary, Ministry of Defence Police, Military Police and the Disclosure Barring Service for England and Wales.
82. Strategic UK governance is exercised through a UK PND User Group (NUG) which is chaired by the UK PND Lead Officer who is the Chief Constable of Durham Constabulary. Beneath this overarching forum sit two other strategic forums and these are the UK PND Business Assurance Group (BAG) and the Non-Standard Services Assurances Group (NAG). The BAG is chaired by the Deputy Chief Constable of Cumbria Constabulary and the NAG is chaired by a Detective Superintendent from the Metropolitan Police. The role of the BAG is to ensure that better information is shared across UK policing services whilst the role of the NAG is to coordinate non-standard service requirements relating to covert policing needs. Police Scotland is represented at an appropriate level on all of these strategic UK policing forums connected with the operation and management of the PND. The overall UK system owner and Senior Information Risk Owner (SIRO) for the PND network is the Chief Constable of Durham Constabulary.

### PND Guidance and Codes of Practice for England and Wales

83. As mentioned under the review of Police Scotland policy relative to PND earlier in this report, there is a range of restricted UK policing guidance manuals which establish rules and conventions on the use of PND. Those of particular relevance to the facial search functionality within PND are the Home Office: PND Facial Searches Guidance 2014 and the College of Policing: PND Search User Guidance 2015. There are also comprehensive training materials and e-learning modules on all aspects of PND.
84. For England and Wales there is also an agreed Code of Practice on the Operational use of PND which was published in 2010 and was presented for adoption through the Westminster Parliament under Section 39A of the Police Act 1996.<sup>38</sup> The Code of Practice sets out the statutory basis for the Code in England and Wales and the role of HM Inspector of Constabulary (HMIC England and Wales) to monitor compliance with the Code, associated guidance and standards.
85. Whilst Police Scotland states that it follows the spirit of the England and Wales approach, there is no Code of Practice for the operation of PND by Police Scotland with a statutory basis in Scotland. As PND is a Home Office system, this means that no legislative authority has been assigned to any external regulator to ensure compliance with any code of practice or associated guidance and standards by Police Scotland. At present, all that exists is the internal audit mechanisms conducted in Scotland by Police Scotland itself, and through wider UK PND audit and accreditation mechanisms established through the PND UK Audit function located within the Home Office.
86. HMICS has previously identified similar concerns around aspects of policing in Scotland not being bound by statutory Codes of Practice that have been adopted on a legislative basis in other parts of the United Kingdom. For example, in our Audit and Assurance Review of Stop and Search published in March 2015 we concluded that the

---

<sup>38</sup> *Code of Practice on the Operational Use of PND, NPIA: 2010.*

introduction of a code of practice would be beneficial in providing guidance in relation to operational practice.<sup>39</sup> This led to a recommendation in relation to a statutory code that was subsequently taken forward by Scottish Government.<sup>40</sup>

87. Whilst noting the statutory responsibilities of the Scottish Police Authority (SPA) to hold the Chief Constable to account for the policing of Scotland,<sup>41</sup> we are unaware of any specific work in Scotland that has sought to provide external assurance over the use of PND by Police Scotland, although we are satisfied from the review that Police Scotland is using PND facial search in an appropriate way. It should also be noted that the National Crime Agency Audit Unit (NCAAU) provides external audit of PND on behalf of the NPCC Lead Officer and reports findings through the UK PND governance structures discussed in the following paragraphs.
88. HMICS recognises the need for independent codes of practice for policing in Scotland as we believe this establishes clearly understood principles and safeguards for the public which are also beneficial in providing clear and transparent operational guidance to police officers and staff. Rather than restrict a recommendation solely to the use of facial images on PND, we conclude that there is an opportunity for Police Scotland and the SPA to consult on and develop a wider code of practice on the use of biometric data in Scotland. As mentioned earlier in this report, primary legislation already exists in Scotland in relation to the retention and use of certain biometrics such as fingerprints and DNA and we conclude that similar legislation would also be beneficial for photographic biometrics held by the police. Whilst it is clear that legality and legitimacy flows from primary biometrics legislation, it is equally the case that the actual policing use including capture, storage, retention, search and disposal by the police service is better controlled by operational codes of practice.
89. The development of such a statutory Biometrics Code of Practice for policing could potentially include fingerprints, DNA and photographs and could be based on existing legislation and existing policing codes of practice in other parts of the UK. This proposed code would require the approval of the Scottish Parliament but such a Biometrics Code of Practice for Scotland could potentially be extended beyond policing to deliver operational safeguards around biometric data held by other public agencies, for example CCTV records and databases. Through review and Parliamentary oversight, such a code would be flexible enough to encompass any new and emerging technologies and legislation.
90. This would help to deliver a wider accountability framework for biometrics in Scotland underpinned by a statutory code, the application of which could be overseen by an independent Scottish Commissioner, (see our Recommendation 2). The Scottish Commissioner could liaise closely with the Biometrics Commissioner for England and Wales whilst recognising his wider locus on matters of UK National Security. Such liaison would also help to address the human rights and ethical concerns that arise from differing UK frameworks being applied to a common UK database, including the issue of Police Scotland having access to information from England and Wales from biometric records arising from circumstances where the retention of such information would not have been permissible under current policy had the record been created in Scotland.

---

<sup>39</sup> HMICS: *Audit and Assurance Review of Stop and Search Phase 1*, paragraph 134, page 46.

<sup>40</sup> Advisory Group on *Stop and Search Report*, Scottish Government, August 2015.

<sup>41</sup> Police and Fire Reform (Scotland) Act 2012, Section 2 (1) (e).



## Recommendation 4

Police Scotland and the Scottish Police Authority should consult with Scottish Government and other stakeholders on the potential development of a statutory Code of Practice for the use of biometric data in Scotland.

### Police Scotland PND governance arrangements

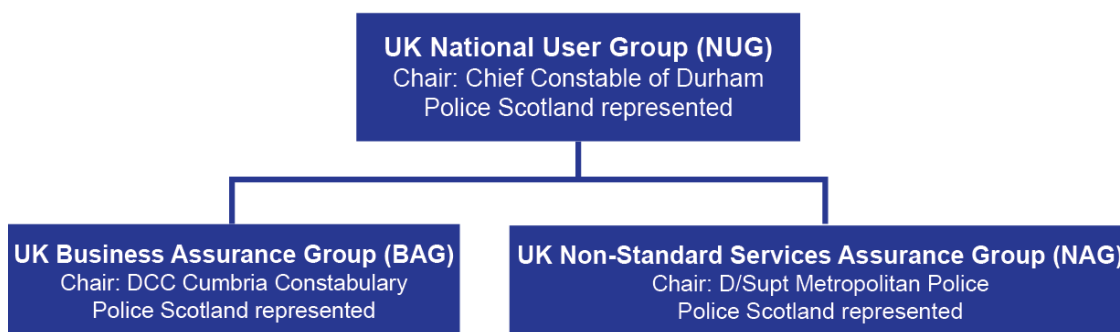
91. The governance arrangements for the operation of PND by Police Scotland are fully described in the Police Scotland SOP. The executive lead for PND and Senior Information Risk Owner (SIRO) is the Deputy Chief Constable Designate. The SIRO is responsible for the risk management accreditation for the use of PND by Police Scotland, and the Force Information Security Office (ISO) reviews information risk management issues and reports to the SIRO through the Information Management Board. There are also two Information Asset Owners for Police Scotland data on PND. These are the DCC Crime and Operational Support for Intelligence data and the ACC Contact, Command and Control, Custody and Criminal Justice for CHS data.
92. The PND system/business process owner is the Detective Chief Superintendent performing the role of Head of Intelligence Support who is responsible for the tactical and operational use of the system by Police Scotland. The Head of Intelligence Support delegates day-to-day responsibility for PND to the Detective Superintendent in charge of Intelligence Support. The Head of Intelligence Support or the Detective Superintendent Intelligence Support co-ordinate arrangements throughout Scotland through a Regional User Group (RUG) on which PND users within the police intelligence community throughout Scotland are represented.
93. All police and Government information systems are required to undergo a formal accreditation process. The National UK Accreditor for Police Information Systems has accredited PND at two separate levels, RESTRICTED and CONFIDENTIAL, which are determined by the integrity level of individual terminals and the environ in which they are sited and must be operated in accordance with the definition of 'Restricted' or 'Confidential' under the Government Protective Marking System (GPMS). Police Scotland PND access points for confidential access are located in confidential environments in accordance with the confidential status of the system or can be accessed at restricted level by an authorised user from any desktop. PND can only be accessed by trained operators normally working in a divisional intelligence, central intelligence support, offender management, or vetting or licensing functions.
94. All PND enquiries are recordable for audit purposes. If the requesting officer is an operational officer then they are required to initially record the reason for the search request in their official police notebook or other auditable format such as the PND Search Request Form and to have the request authorised by a line manager. The Direct PND User will then record the justification and the identity of the requesting officer in the relevant fields within the PND user interface. The PND User also populates a number of other fields which enable the search to be cross-referenced to a relevant crime or incident number. A PND User has authorisation to use PND as part of their day-to-day research activities and as mentioned PND records the reasons for all searches.
95. As part of our audit and assurance review, we examined the governance arrangements in place for the use of the facial search element of PND by Police Scotland and concluded that there are effective governance arrangements in place.



### Police Scotland PND Project

96. In addition to business as usual, there is also an ongoing PND Project within Police Scotland with an associated Project Plan and project management structure. This project remains in existence to oversee the delivery of an automated interface between the Scottish Intelligence Database (SID) and PND. At the moment the interface between SID and PND relies on manual uploads by ICT staff but it is anticipated that an automated interface will be in place by spring 2016, at which point the PND Project will conclude with a business benefits and realisation analysis. The business benefits assessment by Police Scotland at the conclusion on the PND Project will assess success criteria including capturing effectiveness and efficiency metrics as the result of automated processes which reduce the requirement for manual loading of data by police officers and staff. HMICS will monitor the outcome from this work at the conclusion of the PND Project.
97. The following schematic summarises the UK and Police Scotland governance arrangements for PND:

#### UK Governance arrangements for PND





## Police Scotland PND Governance

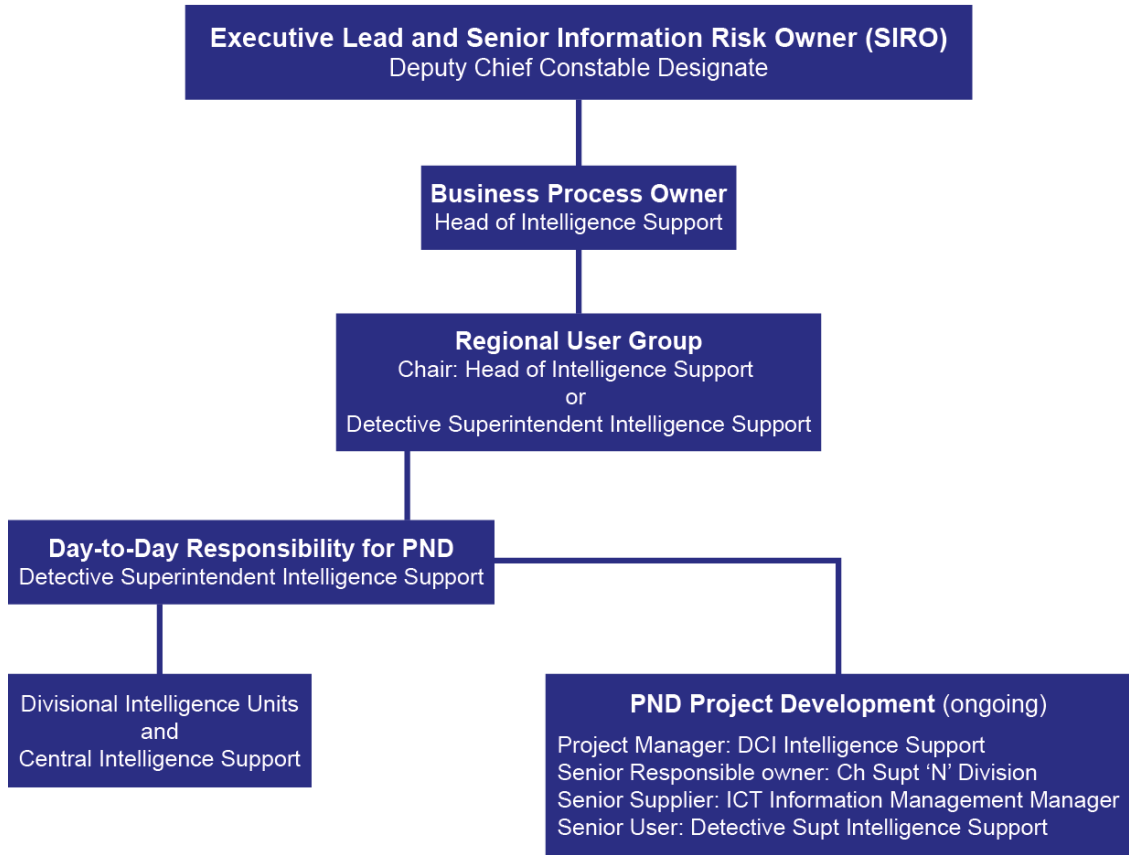


Figure No 1: UK and Scotland PND Governance Schematic

## Administrative and technical interfaces between Police Scotland CHS and the UK PND including weeding and retention of images

---

### The Criminal History System (CHS)

98. In 1960, the first unified Scottish Criminal Records Office (SCRO) was established in Glasgow. By 1987, the first unified police Scottish Criminal History System had been introduced across legacy forces in Scotland by SCRO and initially these criminal records contained only nominal details but by 1995 standard photographic criminal history images had been introduced to all records.
99. The SCRO system was subsequently replaced by the current CHS system which was a legacy policing initiative under ACPOS developed for SCRO and subsequently the Scottish Police Services Authority (SPSA). Records and images on the system were governed by ACPOS and these arrangements included comprehensive retention policies and practices.
100. The operational introduction of PND in Scotland in 2008 was subsequently managed by ACPOS and the former SPSA under legacy policing arrangements. From our review we have established that the key planning decisions in relation to placing Scottish CHS records onto the UK PND in 2011 were made prior to the establishment of Police Scotland and the SPA and this included initial forward planning for the modular updates within PND such as the Facial Search capability. It should also be noted that a criminal history image forms part of a criminal history record and although automated Facial Search on PND did not become available until 2014, Scottish CHS images have been on PND since 2011 and this means that other UK forces have been able to view them since 2011.
101. The Facial Search functionality of PND became available in 2014, and at that time the Scottish CHS records contained 601,837 images of 334,594 people. There were 11.8 million images in PND, meaning that Scottish CHS records accounted for 7.1% of the UK total. The Assistant Chief Constable C5 Division (Contact, Command, Control, Criminal Justice and Custody) is the Information Asset Owner for the operation of CHS by Police Scotland and is supported by National Systems Support in maintaining the integrity of the information held in the system.
102. From our audit and assurance review activities we are satisfied there are effective internal governance arrangements in place around the operation of CHS by Police Scotland. However, as already highlighted in this report there is currently no statutory framework or legislation in Scotland which regulates how the police use or retain photographic images contained within CHS or custody records.<sup>42</sup> There are also no independent external governance mechanisms around the police use of biometrics within the Scottish context.

---

<sup>42</sup> Schedule 2, paragraph 1 (j) of the Police and Fire Reform (Scotland) Act does state that a police custody and security officer has the power to take photographs under the direction of a constable but there is no primary legislation giving a constable the power to take such images.

### **Integrated Scottish Criminal Justice Information System (ISCJIS)**


103. Criminal justice agencies in Scotland have an integrated criminal justice information platform known as ISCJIS. In essence, this involves a process of message exchanges that enables those agencies to electronically access and share information between systems and across jurisdictional lines and to access and share critical information at key decision points in the criminal justice process. In essence, this provides the technical means through which Police Scotland can pass reports to other agencies and it is also the means through which court disposals are received from COPFS and other partners so that police records can be immediately updated. The Police Scotland CHS system is central to ISCJIS.
104. A process map showing the interface between CHS and PND and how these relate to the wider Scottish Criminal Justice Process is included as **Appendix 2** to this report.

### **Administrative and Technical Interface between CHS and PND**

105. CHS is linked to PND over a secure UK police network which enables electronic data transfer between both systems. CHS generates an electronic update to PND at least once every 24 hours and this means that any records created, amended or deleted on CHS by Police Scotland are similarly created, amended or deleted on PND by the following day.
106. In the case of persons who have been charged with a common law crime or statutory offence in Scotland, a pending case record is created on CHS by Police Scotland and the criminal history record and the criminal history image contained therein is automatically uploaded to PND. Once the case has been determined by the prosecuting authorities or courts the relevant COPFS or Scottish Courts disposal is recorded and this in turn generates an electronic notification from the prosecuting authorities through ISCJIS to CHS. In the event of no proceedings or a non finding of guilt, and with the notable exception of statutory provisions for certain sexual and violent offenders, CHS will then remove the record from pending and place it in 'temporary retention' status for up to six months.
107. Data relating to non finding of guilt weeds automatically from CHS and PND after the six month temporary retention period has expired. Whilst the law in Scotland calls for biometric samples to be destroyed immediately in such circumstances, it is important to note that part of the reason for the six month period of temporary retention is to facilitate manual administrative requirements which include such things as destruction of DNA samples, hard copy fingerprints and images. This manual processing is done in response to reports generated from the CHS system. This also caters for circumstances where an accused person is found not guilty of some charges but guilty of others and the complications of rolling and merging cases. In most cases, manual deletion of these materials takes place more quickly. Importantly, it should also be noted that it is not possible for CHS or PND to index an image that is not attached to a corresponding police record so images cannot be retained in either system once a record is weeded.
108. From our audit and assurance review, we can confirm that effective automated processes are in place with regard to the updating of police records and we can confirm that criminal history records and images are updated, amended or removed from CHS upon receipt of decisions from the prosecuting authorities.

### **Police Scotland PND Internal Audit Arrangements**

109. At the time of our audit and assurance review Police Scotland had 134 members of staff trained in the use of PND with 67 active users. As mentioned previously in this report, the authorised PND operators are located in central or local intelligence functions or in related vetting or licensing functions.

- 
110. As part of its internal governance arrangements, Police Scotland has an Information Management function and there are three members of staff who have specific responsibility for conducting internal audits of the use of PND. These three members of staff are located in the three regional command areas of north, east and west. The audit function that these members of staff conduct includes all uses of PND and not just the use of the facial search functionality.
  111. During our audit and assurance review we ascertained that Police Scotland randomly audits 1% of all PND transactions and this culminates in a monthly audit report to management within the National Intelligence Bureau. The results of audits by Police Scotland are also reported to the National UK Auditor and Operational Requirements Board at the Home Office and all force audits are monitored through the UK PND Business Assurance Group.
  112. The actual audit mechanisms involve systems research and direct communication with the original requesting officer to confirm the reasons for the PND transaction and cross referencing to other databases to ensure that the search related to legitimate enquiries about a specific crime, incident or enquiry.
  113. We examined a selection of these monthly audit reports as part of our review and identified no issues or concerns. We are therefore satisfied that Police Scotland has effective internal audit mechanisms in place in relation to the use of PND. However, we believe that the opportunity exists for Police Scotland to share the results of these audits with the Scottish Police Authority in a way that does not compromise the confidentiality of the source data. We have made similar observations in our crime audit and audit and assurance review of stop and search and would therefore encourage the Scottish Police Authority to seek regular updates from Police Scotland on the outcomes from internal audits of PND.

## Comparison with England and Wales

---

### Retention of Criminal Justice Samples in England and Wales 2004 to 2012

114. As discussed previously, the statutory legal framework in Scotland differs from the approach in England and Wales.
115. Prior to the introduction of the Protection of Freedoms Act, 2012, the approach in England and Wales had stemmed from The DNA and Fingerprint Retention Project, jointly funded by the Home Office and the former Association of Chief Police Officers (ACPO) which had been established in October 2003. It was initially set up to deal with the emerging issues that police forces in England and Wales were faced with in implementing the relevant sections of the Criminal Justice and Police Act 2001 and the Criminal Justice Act 2003.
116. Section 82 of the Criminal Justice and Police Act 2001, provided the police in England and Wales with the power to retain DNA and Fingerprints taken from people who were acquitted at court, or not proceeded against. The Criminal Justice Act 2003 was introduced in England and Wales on 05 April 2004. Sections 9 and 10 permitted the taking and retention of DNA samples and fingerprints from all people who were detained at a police station in connection with an arrest for a recordable offence.
117. The extension of legislation to provide for indefinite criminal justice sample retention for all recordable offences in England and Wales was acknowledged as radical, but signalled the Government's intention at that juncture for police forces in England and Wales to utilise criminal justice samples to the full. Whilst acknowledging broader human rights considerations, it is equally the case that retention of all samples offers the potential to match more crime scene materials to potential offenders, improve data quality and achieve cost savings through efficient investigations. However following a subsequent European Court ruling<sup>43</sup> a new biometric regime was established for England and Wales by virtue of the Protection of Freedoms Act 2012. The new regime applies to DNA and fingerprints only and there is no legislation in England and Wales specific to the police retention and use of photographic images meaning that most are retained indefinitely.

### The Protection of Freedoms Act 2012 and the UK Biometrics Commissioner

118. The Protection of Freedoms Act 2012 (PoFA) established a new regime to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints. It also laid down new rules about the retention of such material on UK National security grounds by police forces anywhere in the United Kingdom.
119. The Act also saw the introduction of the Commissioner for the Use and Retention of Biometric material ('the Biometrics Commissioner') whose role is to provide independent oversight as well as to discharge specific casework responsibilities. The Commissioner has a primary focus<sup>43</sup> on England and Wales but also has a wider UK role on matters of UK National security. The new regime was largely introduced by amendments to the Police and Criminal Evidence Act 1984 (PACE). The retention regime established by PoFA in respect of DNA profiles and fingerprints taken under PACE is summarised as follows.<sup>44</sup>

---

<sup>43</sup> S and Marper vs. the United Kingdom (ibid).

<sup>44</sup> Source: Commissioner for the retention and use of biometric material, Annual Report: 2014.



### Convictions:

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

### Non convictions:

Alleged offence	Police action	Time period
All offences		Retention allowed until the conclusion of the relevant investigation or (if any) proceedings. May be speculatively searched against national database.
Qualifying offence	Charge	3 years (+ possible 2 year extension by a District Judge)
Qualifying offence	Arrest, no charge	3 years with consent of Biometrics Commissioner (+ possible 2 year extension by a District Judge)
Minor offence	PND	2 years
Any/none (but retention sought on national security grounds)	Biometrics taken	2 years with NSD by Chief Officer (+ possible 2 year renewals)

Figures No's 2 and 3: Statutory framework for retention of biometric materials in England and Wales under PoFA 2012: Source Biometrics Commissioner Annual Report 2014.

120. In his 2014 Annual Report, the Biometrics Commissioner raised concerns about the use of police custody images and the loading of those images by forces in England and Wales into the PND including those of people who had never been charged or convicted of any offence.<sup>45</sup> The powers of the Biometrics Commissioner only extend to fingerprints and DNA and whilst noting the value of other sources of biometric data to the prevention and detection of crime, the commissioner raised serious concerns that searching technology had been put into operation without public or Parliamentary consultation or debate. He also noted that no other commissioner or regulator appears to have any remit over the use of facial images or facial recognition systems by the police.
121. As mentioned earlier in this report, HMIC England and Wales does have a regulatory function over forces in England and Wales for compliance with the PND Codes of Practice but the Commissioner is making the point that the use of the facial search

<sup>45</sup> This is also a reference to the probe image uploaded for comparison against gallery images.



functionality within PND and the use of probe and gallery images is not the subject of any external regulation in the same manner as applies to the retention of DNA and Fingerprints through PoFA in England and Wales.

In concluding his observations on the matter the Commissioner observed:

“In summary, then, a key and pressing challenge facing Government in connection with new technologies that rely on biometric data is, in my view, the development of an appropriate regulatory regime as regards the application of automated facial recognition technology to police databases of custody photographs. A sensible way of addressing those challenges would be for Government to bring forward proposals for such a regime and to put them out for public consultation. One obvious possible model for such a regime would be that which already applies to DNA profiles and fingerprints.”

(UK Biometrics Commissioner, Annual Report 2014: page 107)

122. In Scotland, the Scottish DNA Database and the Scottish fingerprint contributions to IDENT1 are maintained by the SPA and as mentioned earlier in this report any application by the Chief Constable in Scotland to retain data beyond the prescribed period requires to be made to a Sheriff. Therefore whilst there are different established statutory frameworks for the retention of biometric samples relating to DNA and Fingerprints across the UK, those legislative frameworks do not extend to the retention or use of photographic images.

#### **CCTV Surveillance Camera Commissioner**

123. The Protection of Freedoms Act 2012 (PoFA) also created a Surveillance Camera Commissioner for England and Wales to further regulate the use of public space closed circuit camera systems (CCTV). The role of the commissioner is to encourage compliance with the surveillance camera code of practice in England and Wales, review how the code is working, and provide advice to ministers on whether the code needs amending.
124. The commissioner has no enforcement or inspection powers and works with relevant authorities to make them aware of their duties under the surveillance camera code of practice. As with the Biometrics Commissioner, the general powers of the CCTV Surveillance Camera Commissioner do not extend to Scotland and there is no CCTV Commissioner for Scotland. Accordingly, we conclude that CCTV surveillance cameras could be included within the Biometrics Code of Practice that we are proposing for Scotland.

#### **Political oversight of UK PND by Westminster**

125. The House of Commons Home Affairs Select Committee chaired by Keith Vaz MP is the UK Parliamentary committee which exercises scrutiny over the police use of PND in England and Wales. In January 2015, the committee heard evidence following concerns over the use of PND by British Transport Police on a child protection matter.<sup>46</sup> Concerns were specifically expressed about the failure to upload data to the PND by the force.

---

<sup>46</sup> This was a child protection matter that did not relate to Scotland.

126. The House of Commons Science and Technology Committee have also recently considered the specific issue of Facial Search within PND and current and future uses of biometric technologies and data.<sup>47</sup> The Committee noted the unregulated growth of new technologies and concluded:

*'In the absence of a biometrics strategy, there has been a worrying lack of Government oversight and regulation of aspects of this field. We were particularly concerned to hear that the police are uploading photographs taken in custody, including images of people not subsequently charged with, or convicted of, a crime, to the Police Database and applying facial recognition software. Although the High Court ruled in 2012 that existing policy concerning the retention of custody photograph by the police was "unlawful", this gap in the legislation has persisted. At the very least, there should be day-to-day, independent oversight of the police use of all biometrics. We therefore recommend that the Biometrics Commissioner's jurisdiction should be extended beyond DNA and fingerprints to cover, at a minimum, the police use and retention of facial images'*

(House of Commons Science and Technology Committee, Sixth Report of Session 2014/15, page 3).

127. As a result of parliamentary concerns, it is understood that the Home Office are to commission a review of Facial Search within PND to include an evaluation of success criteria.

#### **Guidance governing the review, retention and disposal of information on UK PND**

128. The review, retention and disposal of material held on the PND is governed by the Guidance on the Management of Police Information (MOPI). The legal framework is set out in section 7 and Appendix 4 of the guidance. This framework applies to information held on any police systems other than the Police National Computer (PNC). In 2015, HMIC England and Wales conducted an inspection of police information management.<sup>48</sup> The report entitled 'Building the Picture' sets out findings from a review of the business processes used in 13 police forces in England and Wales to collect, record, process, evaluate and share information. One of the principal objectives of the inspection was to ascertain if the use of PND was effective and efficient.
129. The HMIC inspection report notes that the PND contains in excess of 1.4 billion records and that on 13 May 2014 it contained 15 million photographic images. It concludes that most forces are transferring information to PND in an appropriate way but that guidance on the retention of information in police systems was not being uniformly and comprehensively applied in England and Wales. This is an important observation by HMIC as the proper operation of a UK database such as PND is entirely dependent on the accuracy and currency of the constituent data that is placed on the UK system by contributing forces.


#### **Other Facial Search Technologies in use in England and Wales**

130. As part of our benchmarking activity with England and Wales we made enquiries with a number of forces and also visited Leicestershire Police to learn about their additional Facial Search technology solution. We have mentioned previously in this report that nine UK police forces do not upload custody images to PND and that Leicestershire Constabulary also has an additional bespoke facial search solution that is not linked to PND.

---

<sup>47</sup> House of Commons Science and Technology Committee, [Sixth Report of Session 2014-15](#).

<sup>48</sup> HMIC Building the Picture: [An Inspection of Information Management 2015](#).


- 
131. Leicestershire Police also uses a Facial Search product known as NeoFace which has been developed by the Japanese technology company NEC, and which is in use by the law enforcement community in many countries around the world. Leicestershire Constabulary chose to use the additional product having formed the view that it offered more advance facial search capabilities than the PND. By adopting a bespoke solution for Leicestershire, the force has control of the quality of the gallery images contained within the system meaning that the system is highly successful when probe images of a similar quality are flushed through the system. However, this success partly flows from having a very small gallery of images against which to search.
  132. The Leicestershire product is not linked to PND and does not therefore search any of the images contained within PND, it solely searches against the forces own records. We were given a demonstration of this system during our visit to Leicestershire and also noted that the searches were conducted by trained identification staff rather than by intelligence staff as is the case in Scotland. We make no observation on this point other than to note broader academic work around 'super-recognisers' where research has suggested that about one to two percent of the population have particular skills in facial recognition. Ordinary people can recognise about 20% of faces they have glimpsed before but super-recognisers can manage 80%.<sup>49</sup> This research may have important implications, for as discussed in this report, neither the PND nor other Facial Search systems in use in UK policing deliver true facial recognition. Instead, the success or otherwise of such systems is to a large extent dependent on a number of variables including image quality and the recognition and investigation capabilities of the staff member conducting the search.
  133. This phenomenon is well known in policing and was recognised by the Metropolitan Police who identified more than 100 super-recognisers within its ranks. Following the London riots in 2011 the force had to trawl through thousands of hours of CCTV images and one officer who was known to be a super-recogniser was able to positively identify 180 of the rioters.

### **Summarising Comparisons with England and Wales**

134. In concluding our brief comparisons with England and Wales it becomes apparent that the commonalities lie in the lack of specific legislation which regulates the use or retention of photographic images by the police. Whilst Scotland has a single criminal history system and weeds records from CHS and PND on non-conviction, this does not happen in the same way in England and Wales due to the absence of an integrated criminal history system or an integrated criminal justice ICT platform. In general, this means that all custody images are retained indefinitely on many police systems in England and Wales and on PND.
135. As discussed throughout this report, Police Scotland only loads a custody image to CHS and PND as a pending case after a person has been charged with a crime or offence. Those images are then deleted from CHS and PND on non-conviction but the corresponding images are retained on Police Scotland custody records in accordance with data retention policies for a period of at least six years regardless of the outcome of the legal process.
136. Contemporary debates on these matters and broader reflections have highlighted the potential need for independent oversight of the police use of biometrics in Scotland, and we conclude that there is transferrable learning from the experience in England and Wales as a result of the safeguards introduced through the independent office of the Biometrics Commissioner.

---

<sup>49</sup> Research conducted by Dr Josh Davis, University of Greenwich.

- 
137. Conversely, national police databases in Scotland and the policies in place mean that police photographic images on CHS are subject of more stringent self-regulation by Police Scotland than is the case with police custody images in many forces in England and Wales. Under final analysis however, there is a significant body of evidence to suggest there are opportunities for improvements in the legislation and regulation of how photographic images and facial search technologies are used by the police throughout the United Kingdom.


## The future direction of biometrics

---

138. As part of our review, we have sought to consider what the future direction may be for the use of biometrics by the police and other law enforcement agencies. From our research, it is clear that the police in Scotland have been using biometrics as a means of criminal identification for more than 100 years. Recent changes in biometric identification for law enforcement purposes are however escalating at pace and international developments include voice recognition, ear prints, and retina and iris scanning. Of particular note is the successful use of hand and vein pattern recognition and its application to the identification of sex offenders based on research by the prominent Scottish forensic anthropologist Professor Sue Black of Dundee University.
139. New and emerging technologies in broader society have also now begun to automate traditional human processes and as a consequence there has also been rapid progress in the use of biometric identification systems and particularly in the fields of international law enforcement and border control.
140. Similar developments have been made with personal technologies and this proliferation includes biometric touch ID technology on mobile telephones and data devices through to biometric identity card systems, iris or retina scanning devices, facial recognition, voice recognition and biometric passports. Whilst many of these technological advances are to be welcomed, there is little doubt that the collection and use of biometric data also presents a number of broader ethical and human rights challenges for society. Such challenges present both opportunities and threats to citizen and state and therefore require careful balance. Key considerations include questions around how such personal data will be protected, and whether highly personal information should be included in unregulated or aggregated databases created by agencies of the state.
141. In February 2015, the House of Commons Science and Technology Committee published a report on the current and future uses of biometric data and technologies.<sup>50</sup> The report covers biometric technologies, development and implementation challenges and legislation and standards. The report noted that three future trends in the application of biometrics had been identified: the growth of unsupervised biometric systems, accessed via mobile devices, which verify identity; the proliferation of “second-generation” biometric technologies that can authenticate individuals covertly; and the linking of biometric data with other types of ‘big data’ as part of efforts to profile individuals.
142. In the report summary, it was noted that each of these trends introduces risks and benefits to individuals, to the state and to society as a whole. They also raise important ethical and legal questions relating to privacy and autonomy. The Committee were not convinced that the UK Government had addressed these questions, nor were they satisfied that it has looked ahead and considered how the risks and benefits of biometrics will be managed and communicated to the public.
143. The report noted the proliferation of biometrics in policy areas such as immigration and law enforcement concluding that the use of biometric data by the state had expanded and would continue to do so. It also concluded that there needed to be more open

---

<sup>50</sup> House of Commons, Current and future uses of biometric data and technologies; *Sixth Report of Session 2014–15*.



dialogue and greater transparency to build public trust and confidence in biometric data and technologies. It was argued that management of the risks and benefits of biometrics was critical and that there had been a lack of oversight and regulation. The Committee were critical of the approach to uploading custody images to PND in England and Wales without public consultation and noted the gap in existing legislation.

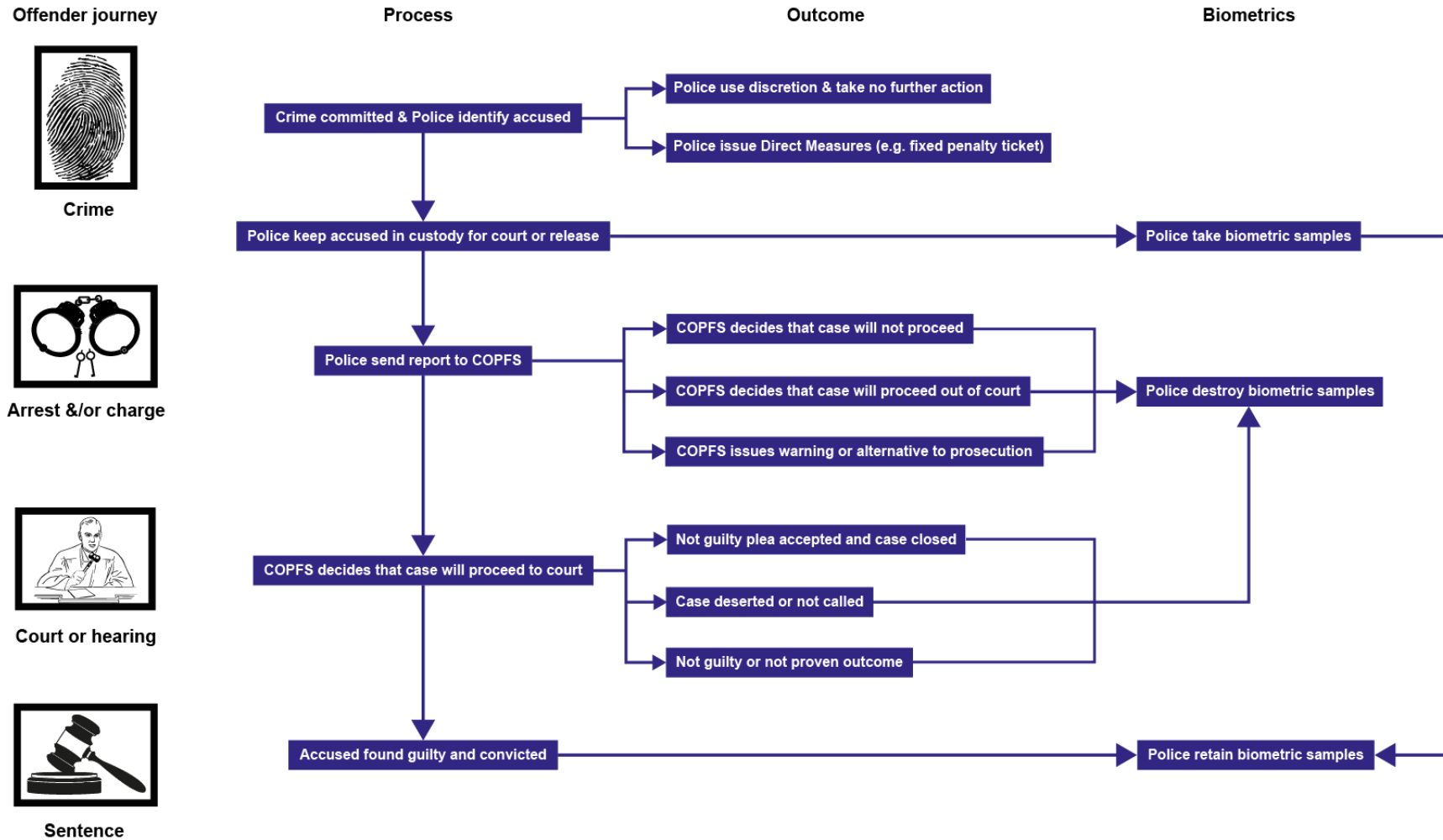
144. Given the current and potential future growth in the police use of biometric data and technologies, the Committee recommended that the role of the Biometrics Commissioner in England and Wales should be extended beyond DNA and fingerprints to cover, at a minimum, the police use and retention of facial images.
145. In a Scottish context, there is clearly a need and expectation that Police Scotland and the SPA will make effective and efficient use of new and emerging technologies so as to fulfil the statutory policing purpose. Whilst we are satisfied from this review that Police Scotland has been making proportionate and necessary use of Facial Search within PND, we have also identified a need for improved legislation and better independent oversight around the police use of biometrics in Scotland. We believe that the establishment of improved legislation and independent oversight will also encourage more open dialogue, greater transparency, and assist in building public trust and confidence in the use of biometric data and technologies by the police. The potential creation of an independent Commissioner to address the issues of ethical and independent oversight of biometrics records and databases held in Scotland also offers the opportunity to provide independent oversight over public space CCTV surveillance cameras and other public space biometrics capture technologies that operate independently of policing in Scotland.
146. Looking to the future, we acknowledge proposals to replace ageing UK policing technologies and to create new UK wide systems. While there may be benefits in Scotland developing its own solutions with the ability to integrate and access a wider UK data pool, we also acknowledge the benefits of Scotland contributing to the development of wider UK systems. However in contributing to UK systems, it is important that Police Scotland has the functionality to administer and maintain Scottish data in compliance with Scottish legislation and any Scottish Codes of Practice in terms of its use.
147. This audit and assurance review has specifically considered the use of the Facial Search functionality within the UK PND system by Police Scotland and has also touched on wider associated issues connected with the police use of biometrics. Our findings are intended to improve police effectiveness and efficiency and as part of this we have also identified some wider opportunities for improvements in legislation and governance. More broadly, we have commented on the scale and pace of technological change around biometrics and forensic technologies and we will be exploring some of these issues further over the coming months when we conduct thematic inspections of Forensic Services and cyber policing as part of our 2016/17 Annual Scrutiny Plan.<sup>51</sup>

---

<sup>51</sup> HMICS *Annual Scrutiny Plan 2015-16*.

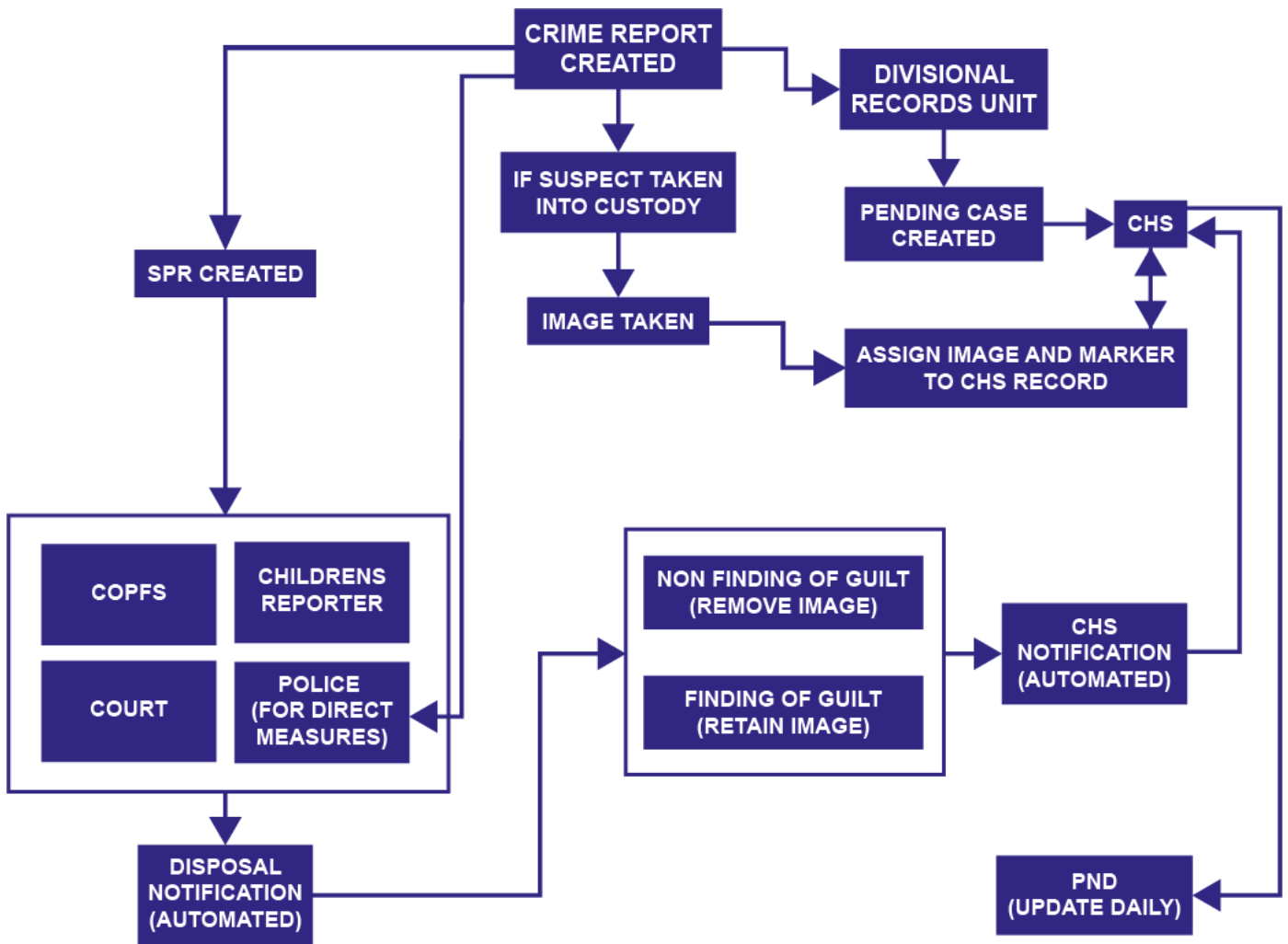


# Appendix 1: Basic overview of biometric sample journey within the wider Criminal Justice Process in Scotland.<sup>52</sup>



<sup>52</sup> This process map does not illustrate the exceptions for DNA and fingerprint retention without conviction in certain cases. See paragraph 29 of this report.

## Appendix 2: Basic Process Map showing technical and administrative interface between CHS and PND in Scotland





## Glossary

---

ACPO	Association of Chief Police Officers (former)
ACPOS	Association of Chief Police Officers in Scotland (former)
APP	Authorised Professional Practice
BAG	Business Assurance Group (PND)
BWV	Body Worn Video
CCTV	Closed Circuit Television
CHS	Criminal History System (Scotland)
COPFS	Crown Office and Procurator Fiscal Service
DNA	Deoxyribonucleic acid
GPMS	Government Protective Marking Scheme
HMIC	Her Majesty's Inspectorate of Constabulary
HMICS	Her Majesty's Inspectorate of Constabulary in Scotland
ISO	Information Security Officer
NAG	Non standard services Assurance Group (PND)
NCAAU	National Crime Agency Audit Unit
NDNAD	DNA Database (UK)
NUG	User Group (PND)
MOPI	Management of Police Information
PACE	Police and Criminal Evidence Act 1984 (England and Wales)
PNC	Police National Computer
PND	Police National Database
PoFA	Protection of Freedoms Act 2012 (England and Wales)
RUG	Regional User Group (PND Scotland)
SCD	Specialist Crime Division
SCRO	Scottish Criminal Records Office (former)
SDNAD	Scottish DNA Database



SID	Scottish Intelligence Database
SIRO	Senior Information Risk Owner
SOP	Standard Operating Procedure
SPA	Scottish Police Authority
SPSA	Scottish Police Services Authority (former)



**HMICS** HM INSPECTORATE OF  
CONSTABULARY IN SCOTLAND

HM Inspectorate of Constabulary in Scotland  
1st Floor, St Andrews House  
Regent Road  
Edinburgh EH1 3DG

Tel: 0131 244 5614

Email: [hmic@gov.scot](mailto:hmic@gov.scot)

Web: [www.hmics.org](http://www.hmics.org)

### **About Her Majesty's Inspectorate of Constabulary in Scotland**

HMICS operates independently of Police Scotland, the Scottish Police Authority and the Scottish Government. Under the Police and Fire Reform (Scotland) Act 2012, our role is to review the state, effectiveness and efficiency of Police Scotland and the Scottish Police Authority. We support improvement in policing by carrying out inspections, making recommendations and highlighting effective practice.

© Crown copyright 2016

ISBN: 978-1-910165-25-6