Scottish Biometrics Commissioner

Assurance Review

of the acquisition, use and retention of images and photographs for criminal justice and police purposes.

Safeguarding our biometric future

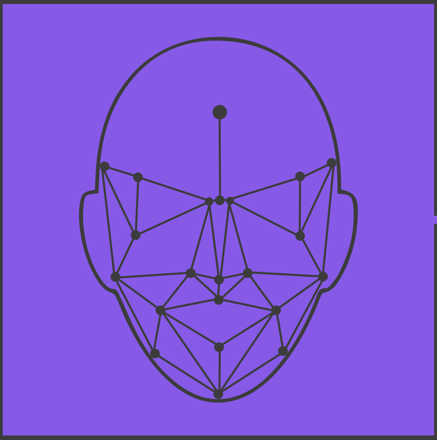
Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Contents

Produced and published by the Scottish Biometrics Commissioner under the provisions of Section 2(3) of the Scottish Biometrics Commissioners Act 2020. Laid before the Scottish Parliament by the Commissioner under Section 20(2) of the Act. SBC/2024/01.

www.biometricscommissioner.scot

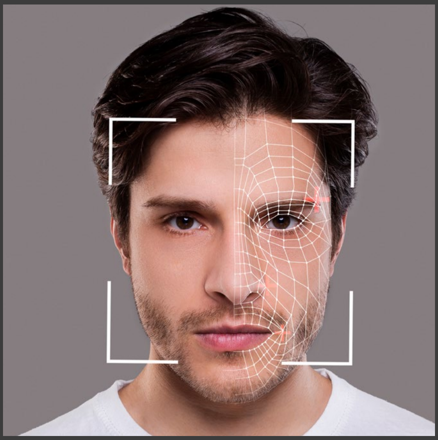
Key facts



Images are used in various ways for policing and criminal justice purposes. Their lawful and effective use makes a valuable contribution to law enforcement and community safety in Scotland.

Police Scotland, the SPA, and the PIRC have no automated means of knowing exactly how many images they have on retention.

There have been no complaints made to the Commissioner from biometric data subjects since the statutory Scottish Code of Practice was approved by Parliament in November 2022.



The Commissioner estimates that there are at least 3 million images held in retention by Police Scotland, the SPA, and the PIRC. However the exact number may be significantly higher.

During 2023 and up to the date of completing our fieldwork in January 2024, no complaints from members of the public have been received by Police Scotland, the SPA, or the PIRC about the use of images or other biometric data.

Strengthening governance will reduce the risk of images being retained for longer than necessary. It will also ensure that other legal obligations such as Freedom of Information, or Subject Access laws are complied with.

Not knowing how many images are held in different databases makes effective governance by each organisation challenging.

Image volumes

The total number of images held in the criminal justice system is unknown, however available figures are:

3 Data volumes

Police Service of Scotland (Police Scotland)

646,935

Images relating to 382,052 people within Police Scotland Criminal History System. However, this number reflects only custody episodes.

The total number of images of all types held is unknown. **We estimate that Police Scotland holds at least 3 million images.**

Scottish Police Authority (SPA FS)

60,000

Forensic Services held approximately eight million images (included master and duplicates) of which c. 60.000 are used for biometric purpose.

The total number of images of all types held is unknown.

Police Investigations and Review Commissioner (PIRC)

54

The PIRC selected June 2022 as sample month for our review. In this month, the PIRC acquired a total of 54 productions. Each of those individual 'productions' could hold a single or multiple images.

The total number of images of all types held is unknown.

?

Total number of images in the criminal justice system is **unknown.**

Police Service of Scotland (Police Scotland)

In September 2023, there were 646,935 images relating to 382,052 people within the Police Scotland Criminal History System. This data is replicated in the UK Police National Database (PND) system. However, this number reflects custody episodes when an arrested person is brought into police custody and charged with an offence. Where persons are arrested but not charged, the police do not capture their image or any other biometric data.

In October 2023, there were 56,158 images on the Violent Sexual Offenders Register (ViSOR) for managed Registered Sexual Offender nominals and another 62,388 archived Registered Sexual Offender nominals managed by Scottish Agencies.

In October 2023, there were 27,996 Police Scotland images in the UK video identification parades electronic recording system (ViPER).

In October 2023, there were 9.5 Tb of data covering 2.000 'incidents' in the camera data and video manager database for Body Worn Video.

Images are also held in a number of Police Scotland systems described further in the report. For these, it is not possible to determine the exact number and location. However, we can **estimate that Police Scotland held more than three million images in 2023.**

Scottish Police Authority (SPA)

In December 2023, SPA Forensic Services held approximately eight million images (including master and duplicates) of which c. 60.000 are used for biometric purposes.

Police Investigations and Review Commissioner (PIRC)

In June 2023, which was used as a sample month for PIRC data, the PIRC held sixteen still images, thirty-four videos and four screenshots for a total of 54 productions that relate to images. Each of those individual 'productions' could hold a single or multiple images. June is considered a typical calendar month in terms of investigations and reviews.

Key Findings

- Images and recordings are the most common type of biometric data used for policing and criminal justice purposes. The exact volumes of such data held are unknown, but significantly outweigh the volumes of all other biometric data types combined.

- Images are used in many ways for policing and criminal justice purposes. Their lawful and effective use make a valuable contribution to law enforcement and community safety in Scotland.

- Unlike DNA and fingerprints which are mostly held in defined databases with automated biometric searching capability, images and recordings are held in different formats and databases including in hard copy.

- The only databases containing images used by Police Scotland with a retrospective and semi-automated facial search functionality are the UK Police National Database (PND) and the UK Child Abuse Image Database (CAID). These are UK policing systems maintained on behalf of the Home Office.

- Police Scotland has never deployed live facial recognition technology capable of mass public space surveillance in Scotland. However, there are circumstances where the future use of such technology should be available to the Chief Constable as a strategic or tactical option for potential deployment. This could include situations where there is a significant threat to public safety or security; threat to life situations, and where such a risk or threat cannot be adequately addressed by conventional policing techniques alone.

- Police Scotland, the SPA and the PIRC have each self-identified opportunities to strengthen their strategic governance arrangements around all biometric data types, including images. For Police Scotland in particular, this is a significant challenge as images cut across all executive portfolios.

- As part of the validated self-assessment on the Code of Practice, and through their own organisational internal audits, Police Scotland, the SPA and the PIRC are making progress in strengthening internal strategies and policies around biometrics, including images.

- During our review, we found that Police Scotland had not yet provided any training to staff on the applicability of the Scottish Biometrics Commissioner's Code of Practice, on the Commissioner's authority to investigate complaints about failure to comply with the Code, and on observing the information rights of data subjects especially where biometrics are obtained without consent, including because of arrest.

- Police Scotland has made some progress in addressing the four recommendations made by the Commissioner in the March 2023 assurance reviews relating to the acquisition of biometric data from children and vulnerable adults because of arrest. However, none of these recommendations have yet been satisfactorily discharged.

- There is an opportunity for Police Scotland, the SPA and the PIRC to improve their internal governance arrangements and to improve the availability of management information on the effectiveness and efficiency of biometric data use so that better information can be placed in the public domain to maintain public confidence and trust.

- Police Scotland, the SPA and the PIRC all have data sharing governance frameworks across agency boundaries which are strong. However, there are circumstances which require further examination. For example - international transfers of biometric data for the purposes of Europol and Interpol where Police Scotland and the SPA Forensic Services have no visibility of when a Scottish record has been shared through UK exchange mechanisms with the European Union and other international jurisdictions. It is however noted that such exchange agreements and their supporting mechanisms are reserved to the UK Government.

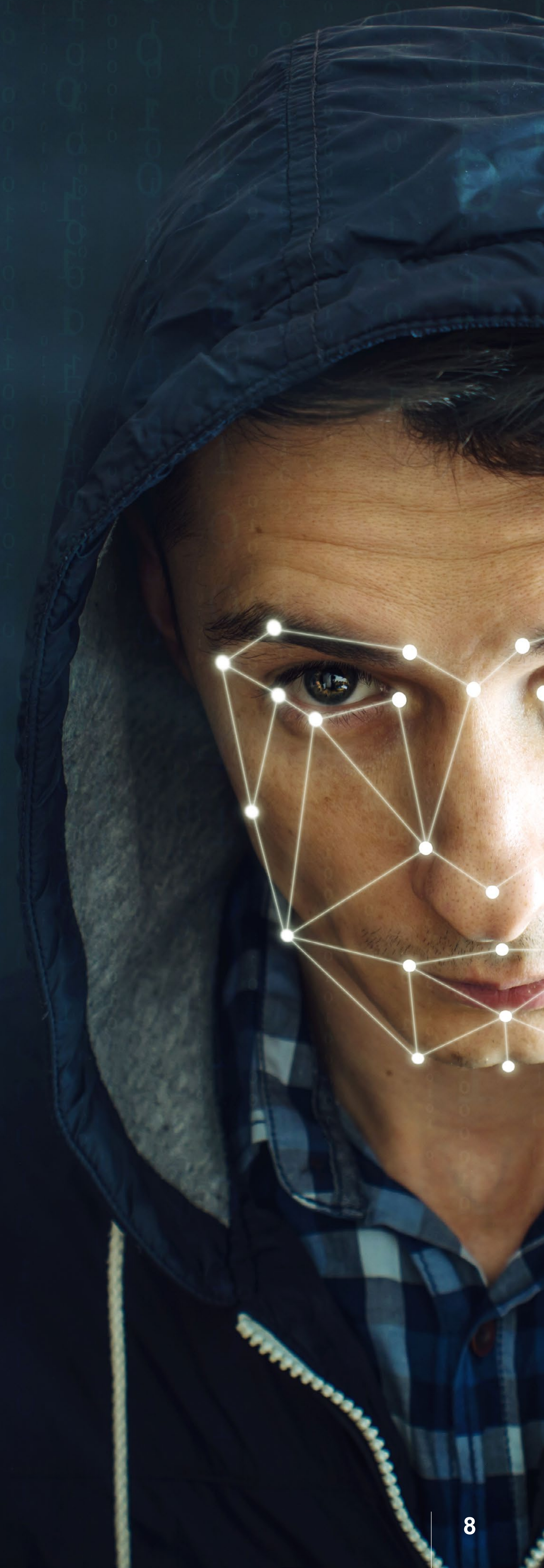
- At the time of our fieldwork, Police Scotland were awaiting legal advice from the UK Information Commissioner (ICO) on whether storing biometric data in the form of images and recordings to the Scottish Government funded Digital Evidence Sharing Capability (DESC) which is hosted on a U.S. headquartered Cloud solution is compliant with UK data protection law.

- The Scottish Biometrics Commissioners Act 2020, and the safeguards of the Code of Practice extend only to Police Scotland, the SPA and the PIRC. This means that oversight of the use of biometric data within DESC extends to some criminal justice agencies and not others. The Commissioner has previously highlighted opportunities to extend biometrics oversight to the entire criminal justice ecosystem in Scotland. However, this is entirely a decision for Scottish Ministers.

- There is a danger that public confidence in the police use of biometric data in Scotland may be undermined by public statements made by the policing minister for England and Wales. The minister stated his desire to give all UK police forces access to the images of 45 million UK passport holders and 55 million photographic UK driving licence holders to enable the images of law abiding citizens to be routinely bulk washed through the apparatus of state surveillance, including police facial recognition.

- The Commissioner welcomes the recent Scottish Government announcement that funding will be made available to Police Scotland to facilitate a national roll out of Body Worn Video (BWV). As previously highlighted by Dame Elish Angiolini in the 2020 review of complaint handling. BWV provides ‘best evidence’ and offers the potential for significant financial savings associated with court attendance, in court proceedings and public inquiries into critical incidents.

- There are no new recommendations arising from this assurance review and the Commissioner is satisfied that Police Scotland, the SPA and the PIRC are currently compliant with the Commissioner’s statutory Code of Practice.



Scottish Biometrics Commissioner

The Scottish Biometrics Commissioner is established under the Scottish Biometrics Commissioner Act 2020.

The Commissioner's general function is to support and promote the adoption of lawful, effective and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by:

- The Police Service of Scotland (Police Scotland)
- The Scottish Police Authority (SPA)
- The Police Investigations and Review Commissioner (PIRC)

The Commissioner has wide ranging general powers and may do anything which appears to the Commissioner to be necessary or expedient for the purposes of, or in connection with, the performance of the Commissioner's functions, or to be otherwise conducive to the performance of those functions.

The Commissioner may prepare and publish a report about any matter relating to the Commissioner's functions.

Produced and published by the Scottish Biometrics Commissioner under the provisions of Section 2(3) of the Scottish Biometrics Commissioners Act 2020. Laid before the Scottish Parliament by the Commissioner under Section 20(2) of the Act.

Definitions

Biometric data

For the purposes of this review the meaning of 'biometric data' is derived from Section 34(1) of the Scottish Biometrics Commissioner Act 2020 which defines the meaning in the following terms:

(1) *…means information about an individual's physical, biological, physiological, or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual.*

For the purposes of subsection (1), "biometric data" may include -

a. physical data comprising or derived from a print or impression of or taken from an individual's body

b. a photograph or other recording of an individual's body or any part of an individual's body

c. samples of or taken from any part of an individual's body from which information can be derived, and

d. information derived from such samples.

Images including facial photographs as described above, are the most common biometric data used for the investigation and prevention of crime in Scotland. Police Scotland, the PIRC and the SPA hold a variety of images and recordings in different systems, databases and often in hard copy. The main databases are described later in this report.

Further reading on biometric data

- A full guide on how biometric data and technologies are used for policing and criminal justice purposes in Scotland has been prepared by the Commissioner.
- An animation video explaining what is biometrics and the role of the Commissioner in Scotland.

Our Assurance Review

This review is a part of a wider programme of assurance activity outlined to the Scottish Parliament in the Commissioners 4-year Strategic Plan laid before the Parliament in November 2021 and then updated in February 2023. The specific methodology for this review was outlined in a terms of reference (ToR) agreed between partners, which was published on the Commissioner's website.

Aims

The intended outcome of this review is to provide assurance to the Scottish Parliament regarding the lawful, effective and ethical use of images used for criminal justice and police purposes in Scotland. For this reason, this assurance review investigated:

1. What is the statutory and policy framework that underpins the acquisition, use and retention of images and photographs for policing and criminal justice in Scotland.
2. Where possible, determined how many images of all types are currently held for policing and criminal justice purposes in Scotland.
3. Described the name and purpose of the various images and photographic databases, including primary, secondary or legacy systems for policing and criminal justice in Scotland such as former force custody or case management systems.
4. Assessed how effectively Police Scotland, the SPA Forensic Services and the PIRC exercise governance and assurance arrangements in place around weeding and retention of images, including when images are transferred to other criminal justice partners and UK databases.
5. Considered what evidence exists to support the value of capturing images and photographs e.g. in terms of crime scene to criminal justice sample match rates.
6. Highlighted good practice and explored any challenges in the use of biometric data by Police Scotland, the SPA and the PIRC.

Exclusions from scope

Biometric data given voluntarily by employees for general employment purposes or where responsibility for regulatory oversight is already vested in another UK Commissioner, including covert surveillance, is not covered by this review.

Methodology

Several qualitative and quantitative methods were used to answer the key aims of this review. The review starts by determining the relevant legislation and policies on images, including photographs used for criminal justice purposes in Scotland. This section covers existing frameworks, available procedures and standard operating procedures relating to images and photographs. Further information on the methodology can be read in the published terms of reference.

The framework used for the assessment is defined below and includes the SBC National Assessment Framework and Code of Practice. Our report includes a data snapshot, where possible, of the volume of data on images and photographs held by Police Scotland, the SPA and the PIRC and detailed analysis of the current practices and governance around collection, use and transfer of this data to other criminal justice partners. Both legal and ethical questions are examined, including the value and purpose of retaining this type of biometric data.

For the purposes of this review, we considered the use of images for all policing and criminal justice purposes by Police Scotland as well as the images used and retained by the SPA and the PIRC.

The legal and policy standards considered for this review were:

- The Criminal Procedure (Scotland) Act 1995
- The Criminal Justice (Scotland) Acts 2003 and 2016
- The Police, Public Order and Criminal Justice (Scotland) Act 2006
- The Age of Criminal Responsibility (Scotland) Act 2019
- The SBC Code of Practice
- SBC National Assessment Framework for biometric data outcomes, which ensures a consistent and objective approach to our work.

Outcomes
Leadership and governance
Planning and process
People
Resources
Partnerships
Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Our National Assessment Framework considers six overarching themes, namely:

🟪 Leadership and governance
🟦 Planning and process
🟪 People
🟩 Resources
🟪 Partnerships
🟨 Outcomes

This assurance review highlights that the volumes of images held by Police Scotland, the SPA and the PIRC is currently unknown by each agency resulting in significant governance challenges. A key finding from this review is that the volumes of images held are significantly higher than the total volumes of all other biometric data types combined. Whilst agencies will often hold several images of the same individual, I would estimate that there are at least three million images being held by Police Scotland.

I wish to extend our thanks to Police Scotland, the SPA and the PIRC staff who assisted our work. Thanks are due to Gillian Jones - Police Scotland Head of Biometrics; Gary Holcroft - SPA FS Head of National Services and Phil Chapman - PIRC Director of Operations for facilitating our assurance activity and information requests. This assurance review and report was conducted by Diego Quiroz, SBC Operations Manager.

Dr Brian Plastow
Scottish Biometrics Commissioner
March 2024

Review of law, policy and practice

This section provides an overview of the legal and policy framework in Scotland in relation to the acquisition, use and retention of images. This includes both a description and assessment of Police Scotland, the SPA and the PIRC internal guidance, practice and governance arrangements. This section also covers an outline of the type of images used and the databases where images are held. We have made an effort to provide data volumes when available.

Legal and policy framework

The primary piece of criminal legislation for biometrics is the Criminal Procedure (Scotland) Act 1995. It authorises the police to take from persons who have been arrested, their fingerprints and DNA. However, the legislation is silent on images or photographs. Nevertheless, it has been customary for more than one hundred years in Scotland for arrested persons to be photographed.

The absence of specific primary legislation in Scotland giving explicit authority to the police to take custody episode photographs is at variance with specific legislative authority in other parts of the UK. This variance has been identified by the SBC Code of Practice, the SBC Children's Assurance Review, Independent Advisory Group on the Use of Biometric Data in Scotland in 2018 and a HM Inspectorate of Constabulary in Scotland (HMICS) Audit and Assurance Review in 2016.

In the case of sexual offences, Section 87(4) of the Sexual Offences Act 2003 provides that the police during the Sexual Offender Notification Requirements could photograph any part of the offender's body. All Registered Sex Offenders must be photographed a minimum of every 12 months, or sooner if their appearance changes.

Notably, Schedule 2 paragraph 1(j) of the Police and Fire Reform (Scotland) Act 2012 introduced a specific provision on images. This provision states that *"A police custody and security officer has power… at a constable's direction, to photograph or take relevant physical data from any person held in legal custody".*

Images and recordings are the most common type of biometric data used for policing and criminal justice purposes and are used in many ways. Therefore, their lawful and ethical use plays a key role for both policing and public trust.

There is an emerging risk that public confidence in the police use of images may be undermined by public statements made by the policing minister for England and Wales in the context of the UK Criminal Justice Bill. He declared the UK government desires to allow police and law enforcement access to the images of 45 million UK passport holders and 55 million photographic UK driving licence holders to run facial recognition checks.[1] The Commissioner has already highlighted the perils of such an approach in his recent opinion piece.

[1] See Guardian article.

Images can be obtained from evidence and acquired from digital forensics. The power to seize evidence from arrestees and suspects is vested in Scots common law, and the term “production” includes photographs, images, recordings and anything else which may be used as evidence in a case. Scotland does not have a Forensic Science Regulator or a forensic science Code of Practice. England and Wales have a Forensic Science Regulator who maintains a statutory Code of Practice. Scots law does not require accreditation for the retrieval of digital evidence, which regularly includes images and recordings. Police Scotland has commenced a programme of work to achieve accreditation of its digital forensic laboratory work by 2025. At the time of writing, most police forces in England and Wales have yet to achieve accreditation of their digital forensic laboratory work.[2]

Images can be used in court or shared with other law enforcement agencies for investigation purposes. The Scottish Government has introduced the Digital Evidence Sharing Capability Service (DESC)[3] which is a digital system that facilitates the sharing of evidence amongst justice partners. While DESC presents an opportunity to improve information sharing, it also raises a number of concerns. One in relation to the independent oversight of the biometric data shared (between those partners) as the Commissioner’s functions are currently restricted to ‘policing’ bodies. Another about the compliance of DESC with data protection laws.[4] The central question for the organisations running this project is whether the use of hyperscale cloud infrastructure provided by U.S. companies is compliant with UK data protection law.[5]
In April 2023, the Commissioner served an Information Notice under Section 16 of Scottish Biometrics Commissioner Act 2020 to Police Scotland due to his concerns. Police Scotland and the SPA have requested advice from the ICO in this respect. At the time of concluding our fieldwork (January 2024) Police Scotland and the SPA were still awaiting advice from the ICO on whether storing law enforcement data to DESC complies with UK data protection laws on international transfers of law enforcement data.

Regarding the retention of images, Scots law is also silent in terms of retention periods.

[2] For example, BS EN ISO/IEC 17025.

[3] Digital Evidence Sharing Capability Service (DESC) is technological initiative of the Scottish Government that will for the first time allow prosecutors, court staff, police officers and defence lawyers to access a unified system to handle evidence digitally. Justice partners and software providers Axon have worked to ensure all the necessary data security and governance for the pilot stage in Dundee.

[4] See for example Computer Weekly article.

[5] Whilst the enforcement of UK data protection law is solely a matter for the ICO, any determination by the ICO that DESC was not compliant would have implications under the SBC Code of Practice. This is because Principle 10 on promoting privacy enhancing technology mandates that biometric data must be protected from unauthorised access and unauthorised disclosure in accordance with UK GDPR and the UK Data Protection Act 2018.

Figure 1. Law, policy and practice

1995

The Criminal Procedure (Scotland) Act is the primary law that gives police authority to take biometrics.

2020

SBC Act receives Royal Assent.

2021

Commissioner appointed – lays first Strategic Plan and Police Scotland establishes Biometrics Oversight Board.

2022

SBC Code of Practice takes legal effect and establishes a presumption of deletion in non-conviction and no-proceedings scenarios providing that the data subject has no previous convictions.

Police Scotland consolidates guidance and establishes a biometrics Standard Operating Procedure (SOP).

2023

Commissioner makes four recommendations to Police Scotland to improve information rights for data subjects, develop distinct policies for children, and improve management information to assist public reporting.

2024

Police Scotland improves their governance structure by appointing Head of Biometrics and new guidance on biometrics.

As a response, the SBC statutory Code of Practice established a presumption of deletion for biometric data [in non-conviction and no-proceedings scenarios providing that the data subject has no previous convictions] following the expiry of the relevant retention periods as prescribed or permitted in law. The Code, which entered into force in November 2022, states that if a biometric data type has no retention period prescribed in law, Police Scotland, the SPA and the PIRC should apply the same retention period as for other types of biometric data, such as DNA and fingerprints in the corresponding case in question.[6]

Overall, the passing of the Scottish Biometrics Commissioner Act 2020, and the adoption of the Code of Practice and Complaints Procedure in 2022 strengthened Scottish accountability and practice by, for example, setting a number of principles for the acquisition, use and retention of biometric data. However, in the rest of the UK accountability is decreasing. The UK government has taken the decision to abolish the role of the Biometrics and Surveillance Camera Commissioner for England and Wales.[7] This is likely to weaken governance and send confusing policy signals across the UK. In practice, it means that except on specific questions of data protection law, there will be no 'independent' oversight of police use of images in the rest of the UK. This is particularly concerning as the National Police Chiefs' Council (NPCC) determined that police custody image storage, deletion and retention is no longer fit for purpose on a national (UK) scale. In January 2024, the Commissioner met with the Temporary Commissioner of the City of London Police, who is the NPCC lead for Information and Assurance to discuss the NPCC findings.[8]

To date it has not been established precisely how many images are held by Police Scotland, the SPA and the PIRC, or where these images are currently held for criminal justice and police purposes in Scotland. The next section outlines, for the first time, the type of images used, the databases where they are held and the numbers of images retained by Police Scotland, the SPA and the PIRC (when provided by the reviewed bodies). This section also provides an assessment of the governance arrangements for each institution.

[6] The issue of retention will be further examined in the upcoming Review of the Laws of Retention in Scotland, which is scheduled to report October 2024. A summary of the aims of the review can be found on our website.

[7] The UK Data Protection & Digital Information (No.2) Bill abolishes the role of the Commissioner in England and Wales.

[8] The Temporary Commissioner of the City of London Police is the Senior Responsible Officer for the improvement programme. The programme aims to support policing by visibly and proactively managing high quality custody images in accordance with law to ensure public confidence and to support policing in making the most effective use of facial recognition for the prevention and detection of crime and supporting the vulnerable.

Police Scotland

Police Scotland was established by the Police and Fire Reform (Scotland) Act 2012 and is responsible for policing across the whole of Scotland. It is the second largest force in the UK with 22,000 officers and staff. In addition to Police Scotland's 10-Year Policing Strategy, which sets the strategic direction and associated outcomes for policing, Police Scotland develops an Annual Police Plan and Performance Framework. Enabler strategies sit under these documents covering Digital, Data and ICT amongst other areas. Local Police Plans for the 13 local policing divisions are also produced every three years. In terms of biometrics, the Assistant Chief Constable for Major Crime and Public Protection is the executive responsible for biometric data. Biometric data and technology however, cuts across all areas of work for Police Scotland.

Practice

In Scotland, and unlike in other UK jurisdictions, Police Scotland only photograph persons in police custody after a decision has been made that they are to be charged with a relevant crime or offence. Persons who are arrested and brought into police custody but who are then released without charge are not photographed unless the image is to be taken for a witness album. This represents good practice by comparison with other UK jurisdictions.

Police Scotland's national custody system itself does not contain images or any other form of biometric data. This differs from the legacy force custody databases which do contain images, including of persons not charged and not proceeded against or convicted. Police Scotland does not have an automated solution to enable the identification and deletion of images retained on its legacy databases.

Police Scotland maintains the Criminal History System (CHS). Legacy databases are being decommissioned, which restricts access to those databases. Images taken of accused persons in police custody settings are uploaded to Police Scotland Criminal History System (CHS) as a pending case. The record and the images in CHS are uploaded automatically to a UK policing intelligence sharing system known as the Police National Database (PND).

It is important to note that Police Scotland will often hold numerous images of offenders who have multiple criminal convictions. This happens as Police Scotland regularly replicates images from CHS into other databases such as the Scottish Intelligence Database (SID), and such images may also be replicated to other locations. For example, when a book of suspect photographs is created from CHS images (or from an arrested suspect) for viewing by a victim of crime during an investigation into a serious crime to assist with potential suspect identification. This means that the same image may exist in primary, secondary and tertiary databases, or locations. This is effective practice as many career criminals regularly change their appearance in an attempt to avoid being identified by the police.

Images can also emerge from digital forensic examinations such as video accepted as evidence or accessed via the various systems available, e.g. body worn video or DESC. At the moment is not possible to determine the data volume for all image databases and systems either managed by Police Scotland or UK agencies.

In the event of acquittal and no previous conviction, the Scottish 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). The management and deletion of images from CHS is manual. This means that no proceeding images are manually deleted. The only automated deletion is in the event of a full CHS records weed.

The age of criminal responsibility in Scotland was raised to twelve years (from eight) under the Age of Criminal Responsibility (Scotland) Act 2019. The Children's Hearings System has become the preferred system for child protection and addresses behaviour including offending. The majority of referrals to the Children's Hearings System are usually made by the police. If a child is referred, their image is retained for the duration of the Children's Hearing case, which is either 2 years for non-sexual or violent offences, or for sexual and violent offences follows Police Scotland's Criminal Record Data Policy.[9]

Police Scotland use a number of Scottish and UK databases and systems (explained below) for criminal justice purposes. Whilst Police Scotland has never deployed live facial recognition technology in Scotland, there are only two databases used by Police Scotland with a retrospective and semi-automated facial search functionality. These are the UK Police National Database (PND), and the UK Child Abuse Image Database (CAID). These systems allow an image or still from a crime scene, incident, or other evidence source (known as a probe image) to be uploaded and compared to a gallery of images of previously arrested persons stored within each database. In each case, the software will return a list of potential matches for further human investigation. The facial search capability within these systems cannot be applied to any other database.

In relation to live facial recognition, the Commissioner has previously stated that there are *'limited circumstances where Police Scotland may wish to consider deploying live facial recognition in future as such technologies improve. For example, in situations where intelligence suggest a very high risk to public safety or security from known individuals, in cases of child abduction involving a threat to life, or when the technology offers the potential to mitigate a serious risk to public safety that cannot otherwise be achieved through conventional policing techniques alone'*.[10]

Police Scotland applies the same retention policy and weeding for fingerprints and DNA to images and photographs. This means that images of persons arrested and not subsequently convicted (and who have no previous conviction) are removed from CHS and PND by Police Scotland as soon as possible. This policy contrasts favourably with the position in other parts of the UK where many forces in England and Wales have been criticised for retaining custody images of innocent people on PND despite the 2012 ruling by the High Court in England that this was unlawful.[11]

[9] Criminal Record Data Policy for convicted case data is threefold: 1. The 40/20 rule means that the subject to whom the data applies must be 40 years old (or over) and the information been on record for at least 20 years (i.e., both conditions must be met) 2. For certain crimes, the 70/30 rule means that the subject to whom the conviction applies must be 70 years old (or over) and the information been on record for at least 30 years (i.e., both conditions must be met), and 3. Convictions will be retained until 100th Birthday for serious crimes.

[10] See SBC operational report 2022/23.

[11] [2012] EWHC 1681 (Admin). More broadly, the UK PND contains over 19 million custody images, and 16 million of these have been enrolled in the facial recognition gallery making them searchable using retrospective facial searching software.

Governance and assurance arrangements around acquisition, retention and deletion

Strategic oversight and responsibility for biometrics rests with the ACC Major Crime and Public Protection. The ACC chairs the Police Scotland Biometrics Oversight Board which meets twice annually and on which Scottish Government, the Commissioner and other relevant partners are included as members. There are also several internal and external governance forums with links to biometrics data.[12] In addition, Police Scotland has a detailed Digital Strategy 2023, which is intended to support the policing outcomes for Scotland through the use of technology and data. The refreshed Digital Strategy aligns to and enables delivery of the agreed strategic outcomes and objectives for policing.

In terms of operational capacity, Police Scotland approved the appointment of two dedicated biometric posts, including a Head of Biometrics in January 2024 to exercise day to day leadership over a complex biometrics landscape which cuts across the portfolios of every Assistant Chief Constable. The Head of Biometrics will drive new Police Scotland strategy, policy, and procedure and will coordinate Police Scotland's response to recommendations previously made by the Commissioner in the 2023 assurance reviews of biometrics acquisition from children and vulnerable adults. The Commissioner welcomes the appointment of a designated Head of Biometrics by Police Scotland.

Police Scotland guidance and policy on images can be found in internal Standard Operating Procedures (SOPs) and Codes of Practice. There are four relevant SOPs and national guidance around acquisition, weeding and retention of images, which are explained below.

Biometrics (DNA, Fingerprints and Facial Images) SOP, Version 1

The taking of criminal justice data (e.g. images, DNA samples and fingerprints) is governed by this SOP. In September 2022, Police Scotland consolidated previous SOP versions and updated this SOP, Section 4 covers facial images. Under this section three types of images can be taken as a part of the custody process: officially accused, evidential and sex offender registration and recertification. The acquisition process for biometric data is the same for both adults and children. The Biometrics SOP is silent on the information that should be given to data subjects during the acquisition process. In our 2023 children and vulnerable adults' assurance reviews we recommended both Police Scotland and the SPA improve the information given to data subjects. Although Police Scotland has made some progress in addressing these recommendations none have yet been satisfactorily discharged. There are no references to the Scottish Biometrics Commissioner Act 2020 or the SBC complaints procedure in this SOP.

Records Retention SOP, Version 5

The SOP's purpose is to define specific retention rules for records held by Police Scotland. It outlines retention periods for custody images loaded to CHS – and then subsequently PND. The SOP is silent in relation to the Scottish Biometrics Commissioner Act 2020 and the Human Rights Act 1998.

[12] These include for example, the internal Biometrics Oversight Board, Police Scotland Audit & Risk Assurance Committee, Data & Retention Oversight Group, the SPA Policing & Performance Committee, the SPA Forensics Committee and the UK Home Office (FINDS Strategy Board).

Body Worn Video for Armed Policing - Code of Practice

The code provides the operational guidance or officers re body worn video (BWV) and supporting digital evidence management. The legislative background cites the relevant law, including data protection law and the Human Rights Act 1998, but there are no references to the Scottish Biometrics Commissioner Act 2020. Note that all footage from BWV cameras is uploaded in the digital evidence management system within the Police Scotland network. Any footage considered nonevidential should be retained for thirty-one days only. Footage identified as evidence is retained according to the Police Scotland Record Retention Policy. BWV footage is shared with third parties when there is a legal basis to do so.

PS Body Worn Video SOP

The guide provides instruction and guidance for officers re body worn video and supporting digital evidence management. The guidance provides equality and human rights considerations as well as references to the relevant law, including data protection law, but there are no references to the Scottish Biometrics Commissioner Act 2020.

The examination of digital devices is now a major facet of modern policing. Learning from past lessons related to challenges in the examination of digital devices,[13] Police Scotland has undertaken a novel approach and ensured that officers and staff responsible for the investigative process are aware of the legal, ethical and human rights implications. For example, the Chief Data Office have introduced a new Data Governance structure for all policing data, including biometrics. When images are extracted using digital forensics tools, including mobile phone extractions, data is stored on a stand-alone secure database using a model that is consistent with digital forensic laboratories across the UK. While accreditation for the retrieval of images is not a legal requirement in Scotland, Police Scotland are working towards UKAS accreditation of their digital forensic laboratory work by 2025.

The governance landscape is complex as Police Scotland uses and stores CHS images on other policing systems with data managed in accordance with the rules applied to that system. This can be illustrated for retention periods. For example, Police Scotland retain images in accordance with their Criminal Record Data Policy or it is weeded 3 years from up to date of death (whichever is sooner). On the other hand, the UK missing persons database weeds images 6 years after the last missing episode, and the video identification parades electronic recording weeds biometric data at 7 years. The Violent Sexual Offender Register does not delete images but archives them when the subject is no longer a ‘managed’ offender - the archived data requires additional authorisation to be accessed by police staff. This means that retention and weeding practice may vary according to the convicted case data or the production evidence schedule.

[13] See for example, Justice Sub-Committee on Policing.

In terms of transfer of images and photographs, Police Scotland have sharing agreements with the following partners:

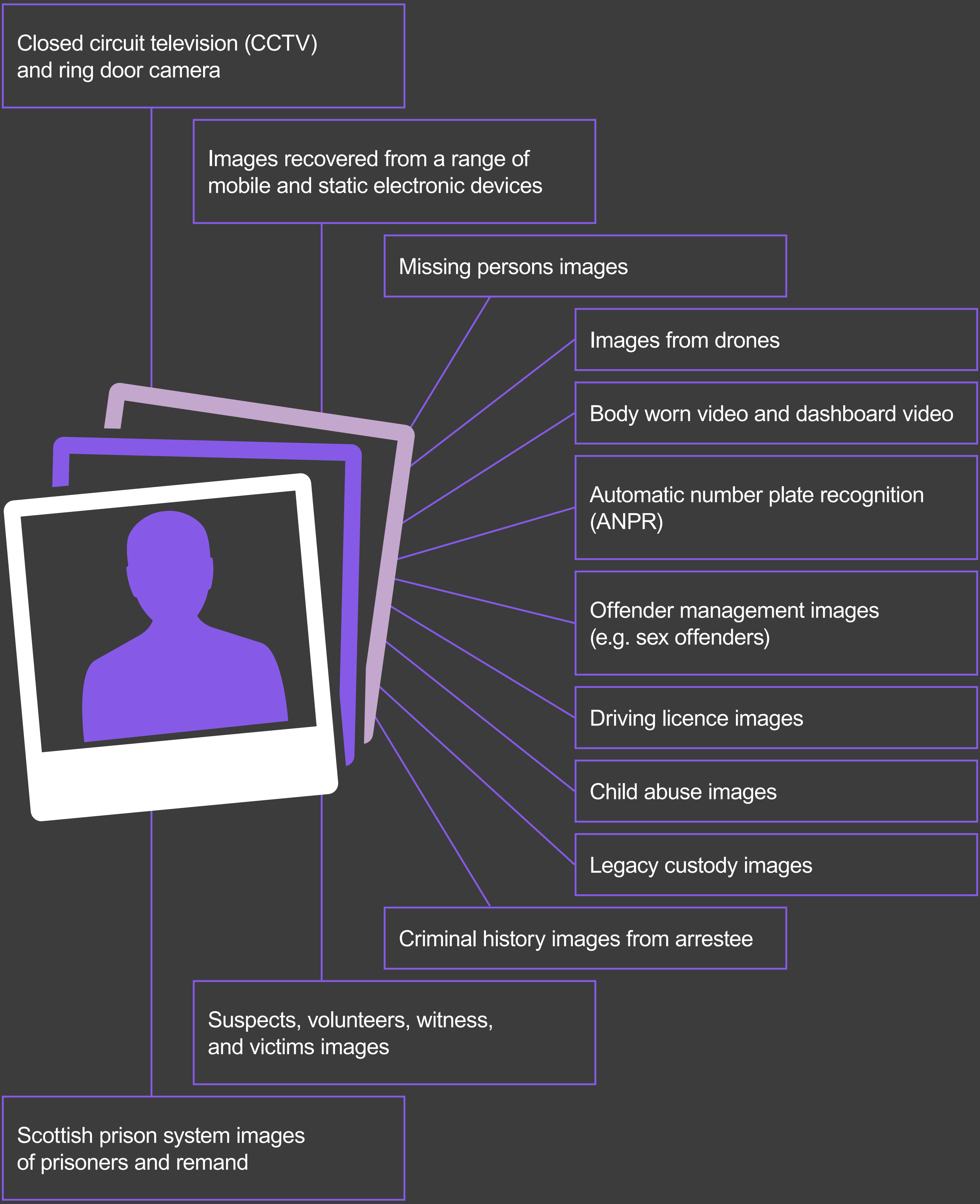
Organisation	Purpose
Crown Office and Procurator Fiscal Service	Evidential
DVLA	Evidential and criminal offences – a view only access to DVLA in connection with the use of a motor vehicle on a road
Forensic Information Database Service (FINDS) / Home Office	Enforcement and investigation purposes. The Home Office is currently considering a proposal to move the oversight of police images in the UK under the strategic governance of FINDS
Other UK forces via PND	Evidential, investigation and enforcement
Europol and Interpol	investigations and international requests[14]
National Crime Agency	Intelligence
UK Prüm[15] via NCA	International crime

Data sharing governance frameworks across agency boundaries are strong. However, in certain circumstances Police Scotland has no visibility of when a Scottish record has been shared or managed, for example with international transfers of biometric data to Europol and Interpol. This is because of the role played by the Metropolitan Police and the National Crime Agency in jointly administering on behalf of all UK police forces the systems for inbound and outbound data sharing between the UK and the EU and other international jurisdictions.

[14] Police Scotland informed that both these agencies weed images at the same time as any instruction for DNA & Fingerprints.

[15] Prüm is an international cooperation agreement between EU members on cross border policing. Since leaving the European Union, the UK has remained aligned with the EU on police cooperation through its trade agreement with the bloc, which replicates the earlier 'Prüm 1' rules. This covers only fingerprints and DNA. The EU is currently negotiating the next version 'Prüm 2', which will include images and the UK will be invited to join it.

Types of images used by Police Scotland[16]



Closed circuit television (CCTV) and ring door camera

Images recovered from a range of mobile and static electronic devices

Missing persons images

Images from drones

Body worn video and dashboard video

Automatic number plate recognition (ANPR)

Offender management images (e.g. sex offenders)

Driving licence images

Child abuse images

Legacy custody images

Criminal history images from arrestee

Suspects, volunteers, witness, and victims images

Scottish prison system images of prisoners and remand

[16] Not all biometric data held by Police Scotland is subject to the Scottish Biometrics Commissioner's legislation, including biometric data that has been obtained under reserved powers (counterterrorism and national security).

Databases & systems where images are held – volumes are presented when provided

- Criminal History System (CHS). Scotland maintains 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 person is brought into police custody and after they have been charged with a relevant crime or offence. 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 PND, so that other UK forces can search the PND to help identify and prosecute criminals. In the event of acquittal and no previous conviction, the records and images are removed from CHS and PND by Police Scotland once notified of non-conviction or absolute discharge by the COPFS.

- Legacy Custody Systems (LCS). Prior to police reform in 2013, the former eight legacy police forces in Scotland made use of five different custody systems. Police Scotland still retain all this data, which will include significant volumes of images of persons not charged or convicted of any crime or offence to reflect the retention policy prevailing at that time. However, Police Scotland has the data locked down so that operational staff cannot routinely access it. Police Scotland is currently in the process of decommissioning these systems.

- Scottish Intelligence Database (SID) is a database now maintained by Police Scotland containing intelligence on people, property, locations and objects. In the case of nominal (people) records, sometimes a SID entry will contain an image of the person to which the intelligence entry relates and sometimes it will not. Any images within SID are used solely for intelligence purposes and not evidential purposes. The Scottish Intelligence Database predates the establishment of Police Scotland. It was originally established by the former Scottish Police Services Authority on behalf of the former legacy forces and the former Scottish Crime and Drugs Enforcement Agency and contains high volumes of legacy images. At the time of the Bichard Inquiry (into the 2002 Soham murders), the Scottish Intelligence Databases was highlighted as good practice in the UK at a juncture when there was little or no effective intelligence sharing between police forces in England and Wales. SID contains copy of arrested for investigation purposes and includes images from the Scottish Prison Service.

- UK Violent Sexual Offender Register (ViSOR) is a national database for the police and the probation service to jointly register, risk-assess and manage sex offenders, dangerous and violent offenders. The ViSOR database will contain a broad array of information, including images. ViSOR is managed by the Home Offices. In October 2023, there were 56,158 images on ViSOR for managed registered sexual offender nominals and 62,388 archived registered sexual offender nominals managed by Scottish Agencies.

- UK Child Abuse Image Database (CAID) is secure database of illegal images and videos of children to aid UK law enforcement. CAID is used as analytical resource to help identify victims and perpetrators of online child sexual exploitation. CAID works by bringing together all the images that the police and NCA encounter, then the police use the images' unique identifiers – called hashes - and metadata to improve how they investigate these crimes and protect children. CAID also supports international efforts to remove images from the internet. CAID is managed by the Home Office.
- UK Missing Persons Database is the national database for all missing person and unidentified body investigations which is managed by the Home Office.
- Driver and Vehicle Licencing Agency (DVLA) database. This database holds more than fifty million driver records and more than forty million vehicle records. The DVLA is an executive agency, sponsored by the UK Department for Transport. Police Scotland view only access can be achieved in connection with a range of police activities connected with the use of a motor vehicle on a road. For example, when dealing with a motorist, a police officer may view the persons driving licence image through a DVLA interface on the officers Pronto digital notebook. This is recognised as effective practice as it removes the need for members of the public to attend at a police station to produce their driving licence if it is not in their possession at the relevant time. Police Scotland does not retain these images. There are other circumstances where the police could access a driving licence or passport image in connection with a criminal investigation, however this can only be done under a specific judicial authority.
- UK Video Identification Parades Electronic Recording (VIPER) is a digital system for conducting identity parades, which is managed by the Home Office and contains images of suspects. The use of virtual video identification parades predates the establishment of Police Scotland, however, is recognised as effective practice which has delivered significant opportunity and cost efficiency savings by comparison with physical identity parades in the pre-digital era. In October 2023, there were 27,996 Police Scotland images.
- Camera data and Video Manager database for BWV. This is a secure internal system for camara data and videos captured by police officers. In October 2023, there were 9.5Tb of data covering 2000 'Incidents'.
- Public space CCTV system is used on public streets and areas across Scotland and include fixed sites as well as non-fixed and rapid deployable CCTV vehicles. The development, management and operation of public space CCTV in Scotland is a matter for local authorities and the police, working in partnership. It contains rolling video rather than individual images.
- UK Large Major Enquiry System (HOLMES). The HOLMES 2 application is the only accredited national application for investigating complex crimes and incidents, providing case, entity and records management features. It is a computer system often containing images and used by the police to manage serious and complex crime investigations. It gives senior officers a real-time view of live operations to help them decide how to best use police resources. It also improves collaboration across all UK forces and other agencies during investigations, helping them find previously hidden links between cases.

- Digital Evidence Sharing Capability (DESC system) is a multistakeholder platform that contains many images for evidentiary and sharing basis, including:
  - Witness image books
  - CHS images
  - ANPR images
  - VIPER images
  - BWV images
  - Drone images
  - CCTV images
  - Images recovered from a range of mobile and static electronic devices and platforms
  - Complainers, victim, and witness images

  As DESC is a multi-agency system used by a range of partners within the criminal justice ecosystem in Scotland, the jurisdiction of the Scottish Biometrics Commissioner and the safeguards of the Code of Practice is partial extending only to the use of DESC by Police Scotland. The SPA and the PIRC do not yet store images or other biometric data within DESC.

- Incident Based Database (iBase) is a standalone IT system used by Homicide Governance and Review Supervisors containing a wide range of information including arrestee images. Police Scotland has recently adopted a policy decision to not store Scottish images on iBase.

- Images are also held in local drives, email boxes and electronic documents within the Police Scotland operating system and network as well as by individual officers, for example images held in the personal digital assistant device or Pronto.

The Scottish Police Authority

The Police and Fire Reform (Scotland) Act 2012 created the SPA and set out its core function, including oversight of policing and holding Police Scotland's Chief Constable to account. The SPA is also responsible for the management and delivery of forensic services in Scotland via the SPA Forensic Services (FS).

The SPA FS is the largest public sector provider of forensic services in Europe providing the full range of forensic services to Police Scotland, the PIRC, COPFS and others. The services include scene examination (e.g. footprints, fingerprints and DNA), chemistry analysis, biology (blood analysis) and specialist services (e.g. handwriting and firearms examinations). There are over six hundred scientists and forensic staff across Scotland, including five main laboratory sites in Aberdeen, Gartcosh, Glasgow, Dundee and Edinburgh.

Practice

SPA FS attended 24,506 crime scenes in 2019/20 and uploaded and managed 3.5 million digital assets on their image management system since the system went live in November 2016, an average of 750,000 per year.[17]

The overwhelming majority of images used and held by SPA FS are the consequence of forensics and include:

- Digital copies of finger and palm print forms for arrestee and elimination subjects
- Photographed friction ridge detail prints recovered from crime scenes, and
- Digital copies of crime scene marks

SPA acquire the productions or evidence from a crime scene or from a police database. Digital forensics is a rapidly evolving area of forensics cutting across all traditional crime types, as well as emerging trends. In this vein is important to note that the SPA FS has highlighted a general lack of adequate funding for ICT solutions.[18] This 'historical underfunding' was also emphasised by both the Commissioner and HMICS in their recent submissions to the Justice Committee's pre-scrutiny budget 2042/25: the HM Inspectorate of Constabulary indicated that the capital allocation to the SPA and Police Scotland has caused the drag on IT development, and the Commissioner expressed concern about the under investment in BWV when compared with all other UK Forces.[19] The Scottish Government has announced that funding will be made available to Police Scotland to facilitate a national roll out of BWV.

[17] SPA FS Forensic Strategy Report 2021/26.

[18] Ibid.

[19] For further discussion on this issue see response to the Criminal Justice Pre-budget scruitny 2024/25.

Governance and assurance arrangements around acquisition, retention and deletion

SPA FS provides oversight, scrutiny and assurance to the SPA through their governance structure at both full meetings of the Authority and committee meetings. This includes biometric issues. The Authority's Forensic Services Committee makes recommendations to the SPA on all forensic services related matters.

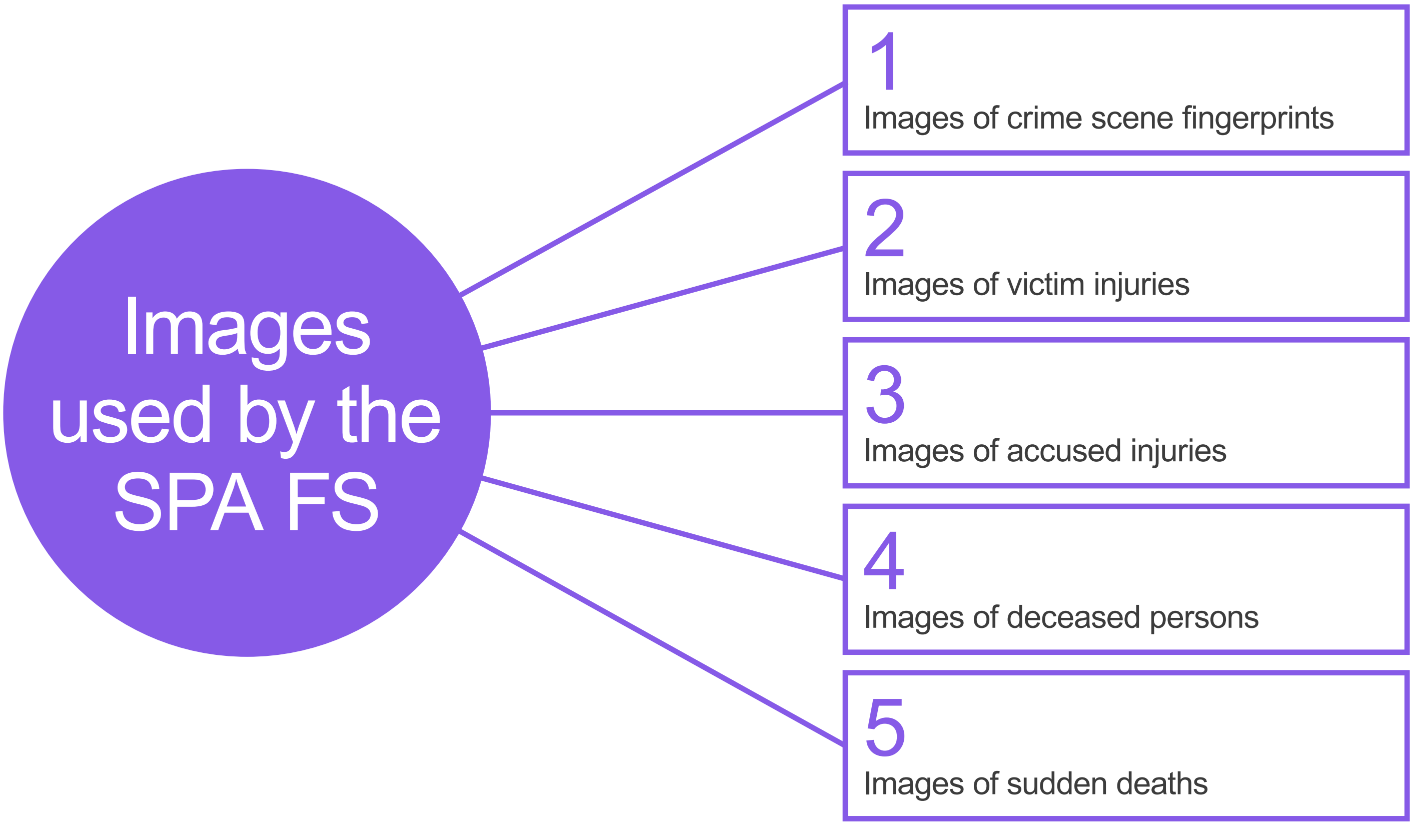
SPA has a comprehensive accreditation and validation processes in relation to the scientific processes they apply to any new technology or forensic method. For example, the UK national accreditation service (UKAS) has granted ISO 17025 accreditation to SPA FS. This accreditation is globally recognised and demonstrates the SPA FS has achieved a level of competence, impartiality and operational consistency.

SPA FS biometrics policy follows Police Scotland's SOPs and Codes of Practice, including on images. The exception is SPA FS internal management system (IMS). IMS is the system where images are stored and is governed by SPA FS Operational Procedure for Scene Examiners. Any image uploaded to IMS is kept as a master copy and duplicates are made for editing, manipulation or other purposes e.g. preparation of evidential image books for court. IMS has approximately eight million images (including master and duplicates).

The SPA FS have 'view only' access to images on CHS and PND as well as to other UK Databases e.g. CAID or ViPER. SPA FS therefore does not manage images on CHS or PND, which means that SPA FS requires explicit instruction from Police Scotland for the retention and deletion of images.

Biometric transfers, particularly on images and photographs include data sharing agreements with the following public bodies:

- PIRC
- Police Scotland
- COPFS - currently being managed as part of the DESC project
- Chief Medical Officer
- Scottish Fire Service



Images used by the SPA FS
1
Images of crime scene fingerprints
2
Images of victim injuries
3
Images of accused injuries
4
Images of deceased persons
5
Images of sudden deaths

Databases & systems where images are held – volumes are presented when provided

- Image Management System (IMS) is an internal database used to store digital images of crime scene marks. IMS holds approximately eight million images (included master and duplicates) of which c. 60,000 are used for biometric purpose as ridge detail images.[20]
- SD cards/laptops/encrypted USB memory sticks - these are used to hold images until a notification has been received confirming successful upload to IMS. Images are deleted after upload to IMS using an assured product.
- SPA Network Drive, which contains legacy images. A governance project is currently working to manage these images – Images can only be accessed with a required authorisation by SPA staff.

[20] The ridge is the anatomical images of the exterior part of a human hand.

The Police Investigations and Review Commissioner

The PIRC investigates incidents involving policing bodies in Scotland and reviews the way Police Scotland handle complaints made about it by members of the public. The legislative foundation of the PIRC is the Police Public Order and Criminal Justice (Scotland) Act 2006 as amended by the Police and Fire Reform (Scotland) Act 2012. During 2022/23, the PIRC received 911 referrals from Police Scotland, COPFS and other policing bodies operating in Scotland. In addition, PIRC was instructed to investigate three complex cases.[21]

Practice

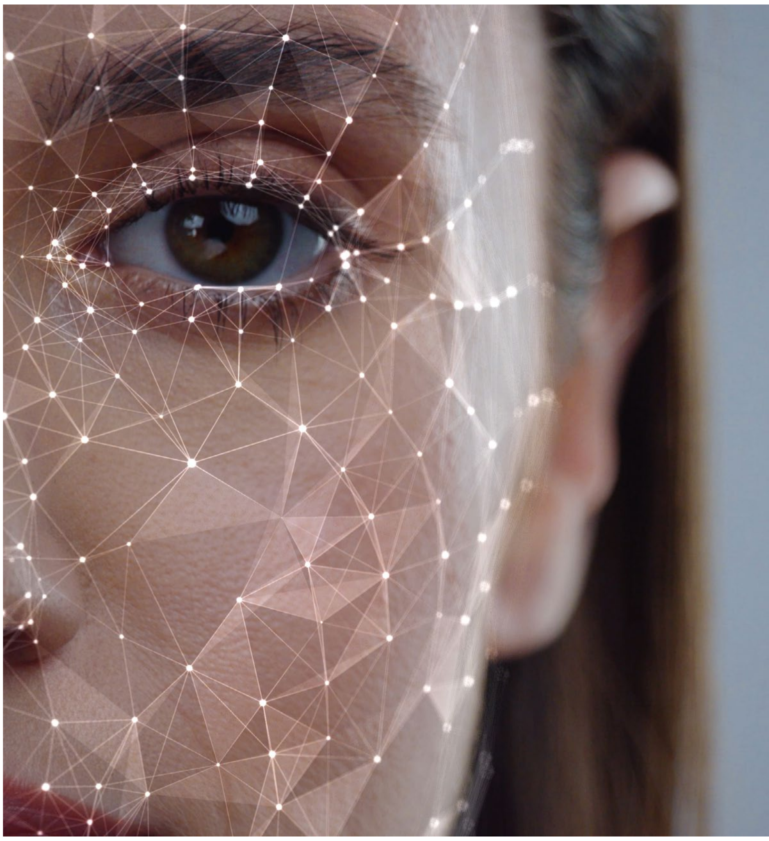
There are diverse ways how the PIRC acquires biometric data. This includes an assessment, an investigation, a CHR and a statutory audit. Typical PIRC investigations involve the seizure of 30-50 productions (or evidence), with medium sized investigations containing 100+ productions, the majority of these being documents or forms.

The most common types of biometric data obtained in the above investigations are CCTV footage, mobile phone footage, still images, voice recordings and medical reports/records which may contain images. Any documents received in hard copy are scanned onto the PIRC system and the originals are shredded (aside from hard copy CCTV footage, original police investigation files or intel records).

The PIRC no longer creates paper files for review applications or police case papers, and although some older case files still exist on paper, the PIRC aims to progress these onto electronic records only.

Most of the information received by the PIRC is held in electronic format. The PIRC receives a significant amount of mobile phone footage and still image files often of injuries, which are sent directly by complainers and members of the public. These are stored in their investigation management software. CHR reports will be kept indefinitely in electronic form as anonymised reports. These will be kept under regular review and are removed when no longer relevant or in the public interest.

The PIRC has limited access to law enforcement databases. The PIRC has a restricted access (view only) and limited resource access to CHS and any information from PNC is sought and provided by Police Scotland.



[21] See the PIRC Annual Report and Accounts 2022/23.

Governance and assurance arrangements around acquisition, retention and deletion

Governance arrangements sits within the regular performance, risk, and finance oversight of the senior management team. This includes biometrics, which is subject to the PIRC's Records Management Policy. The purpose of this Policy is to set out the arrangements for the management, retention and destruction of all data obtained, included images produced and held by PIRC throughout the course of its business.

The PIRC holds an electronic record in the Centurion database for each CHR case, which may include images. The PIRC also hold a print record for each case. However, this practice has been phased out and only cases that pre-date August 2020 (with some limited exceptions) have an associated paper file – which is held in a secure file room. Access to biometric data is restricted to specific and relevant personnel during an investigation or CHR.

The PIRC does not operate, access, use or ingest data to any Scottish, UK, European or international database in respect of images. And while the PIRC can request copies of data held on those databases, they do not have direct access. The PIRC's internal systems, which are described below are standard and lack facial search capabilities.

For investigation and review purposes the PIRC may recover images through digital forensic techniques. While Scots law does not require accreditation for the retrieval of digital evidence, at the time of writing, and in common with Police Scotland, the PIRC staff conducting digital forensic work have received appropriate technical training, but the PIRC digital forensic laboratory work is not accredited to an international scientific standard.

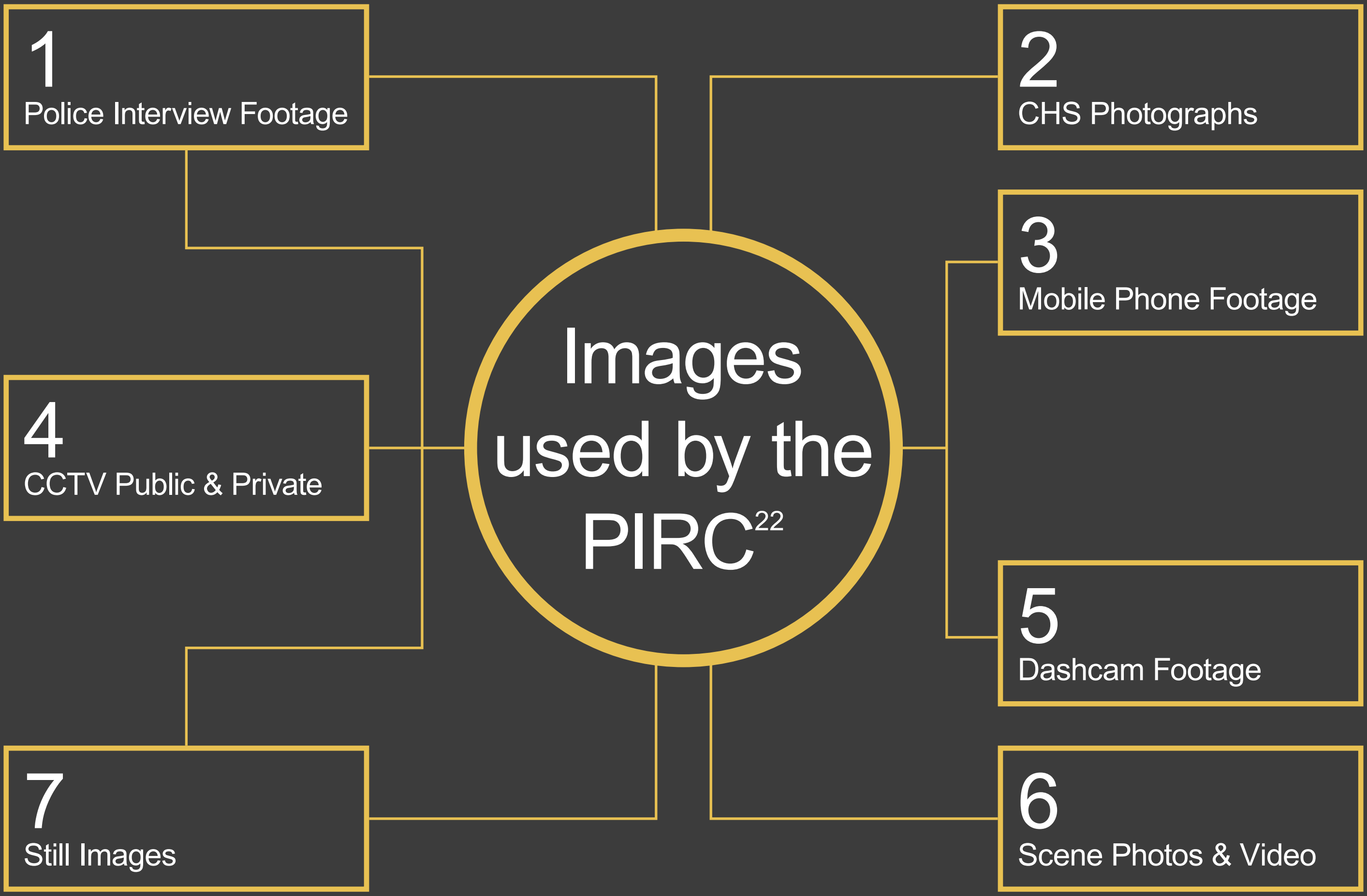
The PIRC rarely acquires, retains and uses biometric data from children. However, the PIRC policy provides that the collection of sensitive data of children (be they arrested persons or witnesses) should only be performed when necessary and following discussion with the lead investigator (of at least the rank of Deputy Senior Investigator).

Notably, the PIRC's Records Management Policy explicitly references the Scottish Biometrics Commissioner Act 2020 and the obligation to comply with the SBC Code of Practice when recording, storing, processing and destroying biometric information in relation to their role within the criminal justice field. All biometric data is subject to this policy.

The PIRC does not apply different retention periods to images, compared to other biometric data. Most retention periods follow the CHR file and relevant conclusion schedule for the purpose the material was collected. For example, in respect of Reviews Case Materials, the PIRC will retain the electronic file for a period of 3 years from the date the CHR is issued or the recommendations/reconsideration directions are implemented/completed (whichever is later), and no less than 12 months from the date of the last action, correspondence or contact on the file. In respect to Criminal Investigations where the subject is prosecuted by summary proceedings, the electronic record including productions will be retained for 5 years and in cases dealt with under solemn proceedings, electronic records (and hard copy) will be retained for 10 years from disposal of case. For 'material' relating to Police and SPA referred investigations, which may include images, the PIRC will retain the data for 3 years following the conclusion of the investigation.

Monthly identification of eligible records to be disposed is conducted by the PIRC's Admin Officer who will ensure that there are no outstanding matters before the file is weeded. In certain cases, electronic files (including images) may be retained at the PIRC's discretion, for example where the case has set a precedent or any case of public interest. Such cases will be reviewed annually to determine whether retention of the file remains necessary.

In terms of transfers of images and photographs, the PIRC exchange material with British Transport Police (usually body-worn video and CCTV footage) via their NICE software/platform with a time-limited access. Transfers are also exchanged with Police Scotland and members of the public using Egress, which is the PIRC's secure online file sharing platform.



Databases & systems where images are held – volumes are presented when provided

- **CLUE2 and CLUE3.** These are investigation management software contained within standalone systems. They are the PIRC's primary investigation software and database. CLUE3 replaced CLUE2.[23] CLUE3 is the main database for storing information relating to an investigation, including images and videos.
- **CENTURION** is the case recording and management software used by the PIRC's reviews staff when dealing with CHR. Files are not stored in this system, Centurion is used as an interface for managing the data.
- **'S' Drive**. CHR files and data are stored on this drive, which is a network on the Scottish Government's secure SCOTS operating system. The 'S' Drive can only be accessed by the PIRC's reviews staff, management, and administration personnel.
- **Egress** is a security online platform, which the PIRC uses to exchange information and data with Police Scotland and members of the public. Examples of usage include video clips, images and medical records which may contain biometric data. The Egress administrator rights are limited to technical investigators.

[22] Note: not all biometric data held by PIRC is subject to the Scottish Biometrics Commissioner's legislation, including biometric data that has been obtained under reserved powers (counterterrorism and national security).

[23] There are still files retained in CLUE2 due to timescales involved for some criminal cases.

- Sonology is a Network Attached Storage (NAS) system which is effectively a private cloud that is not web-based. It is a centralised location that allows the PIRC to 'back-up' essential files and store large files that are either too large to store on the 'G' Drive', or that are so large (i.e. high-definition videos) that require to be 'off network' so that processing speed is not affected. Access to the Synology is restricted to a limited number of staff and is administered by the PIRC's technical investigators.
- Investigations 'G' Drive is a network drive on the Scottish Government's secure SCOTS operating system where most of the Investigations Department case files are stored. Some of these files may be uploaded on and duplicated from CLUE3.
- Manual records and Productions Store which contain hard copies of images or disc containing the original digital image.

The PIRC currently has no automated means of knowing how many biometric records it holds. It is also not possible to provide an estimated figure as retention policies vary according to the reasons why the PIRC hold certain data. However, the PIRC undertook a sample month's inventory of images held for this assurance review.[24] The sample returned sixteen still images and thirty-four videos and four screen captures for a total of 54 productions that relate to images for cases started in June 2022. Each of those individual 'productions' could hold a single or multiple images.

As part of internal proposals to improve biometric data governance, the PIRC plans to explore a technical solution to enable all records containing biometric data to be tagged. This would significantly improve the availability of management information on biometric data held by the PIRC.

Figure 2. Summary of biometric data by type obtained by PIRC in June 2022

Biometric Data Type	No.
CCTV Footage	26
Mobile Phone Footage	8
Screen Capture	4
Scene Photograph	-
CHS Photograph	-
Still Image	16

Department Held by	No.
Investigations	15
Reviews	3
Art 3 Assessments	36
Corporate Services	-
Communications Dept.	-

[24] A total of 54 items were assessed as containing biometric data held within images by the PIRC within the sample month. These related to incidents that were assessed, or Investigations or Reviews that commenced, during June 2023. June 2023 is considered a typical calendar month in terms of investigations and reviews.

Strategic conclusions

This review aimed to provide for the first time, a clear picture of the current landscape on the use of images in Scotland. For this purpose, the report describes the current legal and policy framework and identifies the type and location of images in existing databases. It was clear from the initial stages of the review that establishing the total data on volumes of images was not going to be feasible due to the constrains outlined in this report. However, this report explores the available data. To understand the current landscape, it was also crucial to define the institutional governance for the acquisition, use and retention of images. In doing so we have assessed institutional procedures, identified good practice and underlined areas for improvement. We hope this report also contributes to increase public confidence and democratic oversight of biometrics and how it supports law enforcement agencies in Scotland.

Unlike DNA and fingerprints which are mostly held in defined databases with automated biometric searching capability, images and recordings are held in different formats and databases including in hard copy. This creates risks as well as governance and control framework challenges for the reviewed bodies.

There has been a lack of adequate funding for ICT solutions, which underpins the images application landscape. This 'historical underfunding' was highlighted by the SPA FS in their Forensic Strategy 2021. Both the SBC and HMICS have also highlighted the funding issue in their recent submissions to the Justice Committee's pre-scrutiny budget 2024/25.

The Scottish Biometrics Commissioner Act 2020 together with the SBC statutory Code of Practice and the Complaints Procedure have contributed to strengthen accountability in Scotland. This contrasts with the position in the rest of the UK where decisions such as abolishing the Biometrics and Surveillance Camera Commissioner for England and Wales are weakening independent oversight, democratic accountability and good governance.

From both the interviews and the documentation provided by Police Scotland, the SPA and the PIRC it is clear that biometrics governance is on a journey of change and improvement. There are several examples of good practice within the reviewed bodies, including in-house gap analysis on biometrics; the ongoing revision of internal policy and guidance; the development of new guidance on images (and other biometric data), and the announcement of new structures around biometrics, including a Head of Biometrics for Police Scotland in January 2024.

However, no overarching strategy has been implemented across both Police Scotland and the SPA FS who jointly administer the arrangements for managing Scottish DNA and fingerprint records and in certain circumstances images. Consequently, it is difficult to clearly determine overall aims and each of the organisations' separate or joint responsibilities in respect of the management of images and other biometrics. We endorse the development of a joint strategy statement for the acquisition, use, retention and destruction of biometric data with separate biometric strategies for Police Scotland and the SPA FS. This strategy should have explicit references to our legislation and explain how it will contribute to wider outcomes, such as criminal justice, and the National Outcomes for Scotland.

In strengthening strategy and policy around biometrics, we also suggest the provision of relevant training for staff, particularly on the applicability of the Scottish Biometrics Commissioners' Code of Practice; on the Commissioner's authority to investigate complaints about failure to comply with the Code and on observing the information rights of data subjects.

In parallel with this assurance review and report, the Commissioner conducted the first annual assessment on compliance with the SBC Code of Practice. All three reviewed bodies were found compliant in January 2024.

We continue to be concerned about the lack of information provided to data subjects – whether arrestee, victim or witness. The internal guidance examined is mostly silent on information rights and good practice. There is no requirement for operational staff to provide any meaningful information to data subjects explaining the reasons why their images or other biometric data is to be captured following arrest; or any explanation of where the data will be hosted; what the data will be used for; who it will be shared with; how long it will be kept or any appeal mechanisms to Police Scotland, including references to the SBC Code of Practice and Complaints Procedure.[25] This is particularly important when acquiring images and photographs of vulnerable people.

[25] See SBC assurance reviews and recommendations.

The total data volumes of images is unknown and not easily accessible or possible to determine. While all reviewed bodies can identify the type of images acquired and held in their systems, total volumes are unknown. Exact locations of images can only be defined for automated systems. Police Scotland can determine data volumes related to images for CHS and a few other databases. The SPA cannot determine the exact volume used for biometric purpose but can identify the types held. And the PIRC can determine the types of biometric data held in their inspections and investigations but cannot determine the exact number of images they hold. This renders the governance of this type of biometric data partial. A historic analysis of the available volumes, presented in our Operational report 2022/23, shows that volumes are generally increasing year by year.

All reviewed bodies give due consideration to data protection, for example, by systematically undertaking data protection impact assessments as a part of adopting new technologies. However, it is also important that relevant policies and procedure are subject to a Community Impact Assessment (CIA), and an Equality and Human Rights Impact Assessment (EQHRIA) as per principles 4, 5, 8 and 11 of the SBC Code of Practice.[26]

There are only two databases with retrospective facial search capability. These are the PND and CAID, which are owned by the UK Home Office.

There are concerns around the necessity and proportionality of retention policies for images. Police Scotland and the SPA have established a weeding and retention practice for convicted persons, which follows CHS conviction retention periods. This means that there is a risk that images could be retained longer than necessary.[27] All reviewed bodies are aware of this issue. Police Scotland's work on deletion of images not linked to a live prosecution or conviction is ongoing.[28] The SPA FS has introduced a manual workaround to ensure weeding is compliant with the 1995 Act and the SBC Code of Practice. The PIRC is planning to adopt a technical solution to enable all records containing biometric data to be tagged. All of this would significantly improve the availability of management information on biometric data held.

The issue of retention will be further examined in the upcoming Review of the Laws of Retention in Scotland, which is being conducted in partnership with Scottish Government and which is scheduled to report in October 2024. An outline of this review and the key areas to be examined can be found on our website.

Police Scotland and the SPA FS data sharing governance frameworks across agency boundaries is strong. However, there are circumstances which require further examination related to the international transfers of biometric data for the purposes of Europol and Interpol where Police Scotland and the SPA Forensic Services have no visibility of when a Scottish record has been shared. This is however a reserved matter in the UK.

[26] Our Assessment Framework - quality indicators for biometric data explicitly recommend related to governance (B3) that 'Data security, community impact, equality impact, and privacy impact assessments are conducted in respect of biometric data and technologies ensuring that ethical and human rights considerations are embedded into operational practice and policy'.

[27] The European Court of Human Rights (ECtHR) has engaged with several judgments concerning the collection or retention of biometric data, which have clarified and developed the standards for the use of DNA, fingerprints, and photographs in criminal justice. For example, in Gaughran v. the UK (2020), the Court called into question the extremely extensive scope of the data retention system.

[28] Approximately 40.000 images have been identified for weeding by Police Scotland Digital Division by December 2023.

There is an opportunity for Scottish Ministers to consider whether the functions of the Commissioner and protections of the Code could be extended to include where biometric data is used by a range of other actors, including for DESC and public space CCTV systems. The current protections of the Code of Practice do not extend to public space CCTV - other than any use by Police Scotland, the SPA or the PIRC. These concerns have been highlighted by the SPA chair and the Commissioner who called for a more coherent approach to the oversight of public space CCTV images in Scotland.

Police Scotland, the SPA and the PIRC hold extraordinarily little management information on image volumes including any metrics pointing to their effectiveness. This was the subject of a previous recommendation to Police Scotland in the Commissioner's assurance reviews relating to children and vulnerable adults in March 2023. Police Scotland and the SPA FS produce joint statistics for DNA on the SPA's website. There is an opportunity for Police Scotland, the SPA and the PIRC to consider what additional management information (quantitative or qualitative) on images and other biometric data could be safely placed in the public domain. This would help to demonstrate the effectiveness of that data within the criminal justice system to better inform public understanding and maintain confidence and trust in its use. The SBC Code of Practice requires engagement with the public and other external stakeholders as an integral part of planning and improving services.

In 2021, research conducted on behalf of the Scottish Biometrics Commissioner by ScotCen showed high levels of public confidence in the use of biometric data by Police Scotland. However, there is a significant risk that public confidence in the police use of biometric data may be undermined by public statements made in other jurisdictions. In this report we highlighted the policy position of the policing minister for England and Wales. The intention is to give all UK police forces access to the images of 45 million UK passport holders and 55 million photographic UK driving licence holders to be routinely bulk washed through the apparatus of state surveillance, including police facial recognition.[29] The Commissioner strongly opposes this policy.

[29] Reported in the Guardian on 21 Dec. 2023 'Surveillance Britan', and on 29 Oct. 2023 'Police Urged to Double Use of Facial Recognition Software'.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

Safeguarding our biometric future