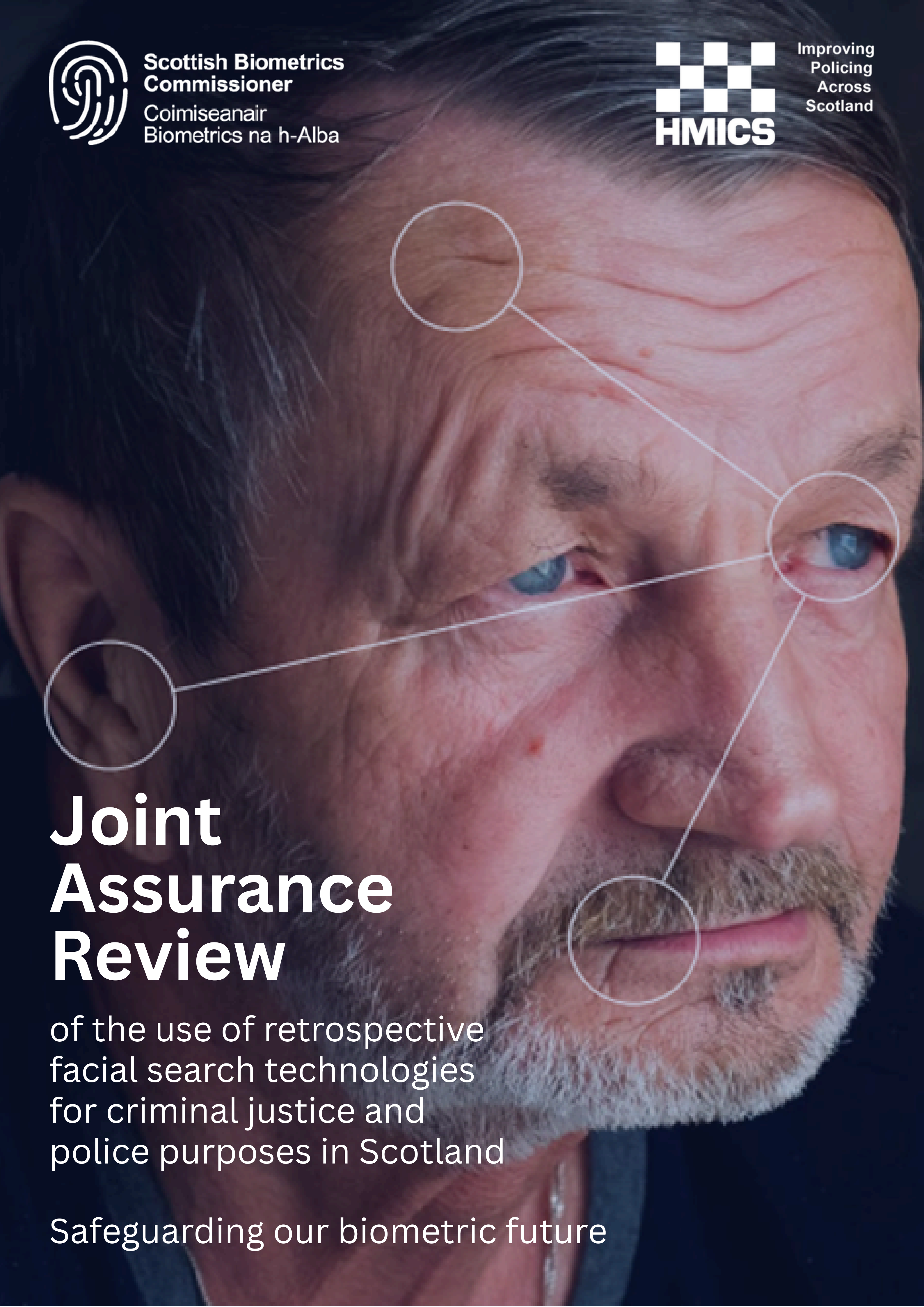


Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

HMICS
Improving Policing Across Scotland

Joint Assurance Review

of the use of retrospective facial search technologies for criminal justice and police purposes in Scotland

Safeguarding our biometric future

Table of Contents

2 Key facts

4 Key findings

7 Summary of recommendations

9 Chapter 1. Introduction to our assurance review
- The Scottish Biometrics Commissioner and partners
- Aim
- Methodology and scope

14 Chapter 2. Definitions
- What is biometric data
- What is retrospective image search
- Why PND and CAID

17 Chapter 3. Law and policy
- The law and internal policy
- PND Governance
- CAID Governance

28 Chapter 4. Evidence gathering and findings
- Interviews with Police Scotland and onsite visits
- Data volume return 2023-24
- Comparative data (PND)
- Sanitised cases

43 Chapter 5. Future legal and ethical challenges

Produced and published by the Scottish Biometrics Commissioner under the provisions of Sections 2 and 3 of the Scottish Biometrics Commissioners Act 2020 – SBC/2025/02. Laid before the Scottish Parliament by the Commissioner in March 2025 under Section 20(2) of the Act.

SBC/2025/02

www.biometricscommissioner.scot

Key facts

Retrospective Image Search Technology (RIST) is used in two databases in Scotland: Police National Database (PND) & the Child Abuse Image Database (CAID)

PND is a national UK policing information and intelligence sharing system, which has a facial search functionality. Police Scotland has 'live access' to the PND system

CAID is a UK policing secure database with a facial matching functionality of illegal images and videos used to identify victims and perpetrators of online child sexual exploitation. Police Scotland periodically upload images to the CAID system

Police Scotland has an **automated means of knowing** exactly how many retrospective image searches are run for a period of time

PND = There were **3813 facial searches** for 2023-24 (April to March)

CAID = There were **193 facial searches** for 2023-24 (April to March)

The evidence suggests that **RIST plays an important role in law enforcement** investigation and community safety in Scotland. RIST overall quantitative contribution to policing is very low

There are strong safeguards for its use, however, Police Scotland holds no management information on the **effectiveness** of Retrospective Image Search Technology

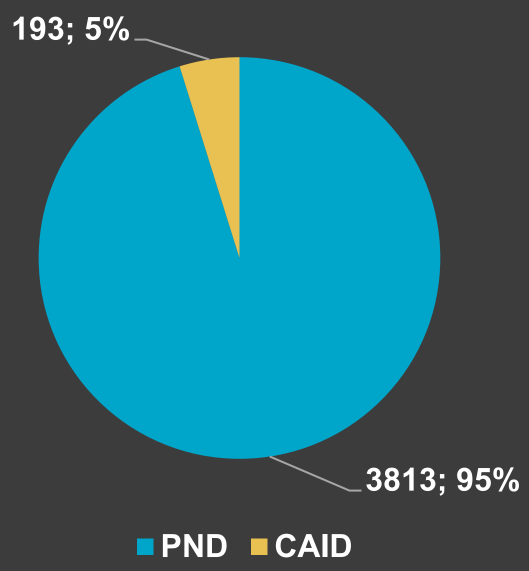
Strengthening this together with improved governance will help Police Scotland keep its effectiveness and legal compliance under review

During the 2023 -24 financial year and up to the date of completing our fieldwork in January 2025, **no complaints** from members of the public have been received by Police Scotland, about the use of RIST

Key facts

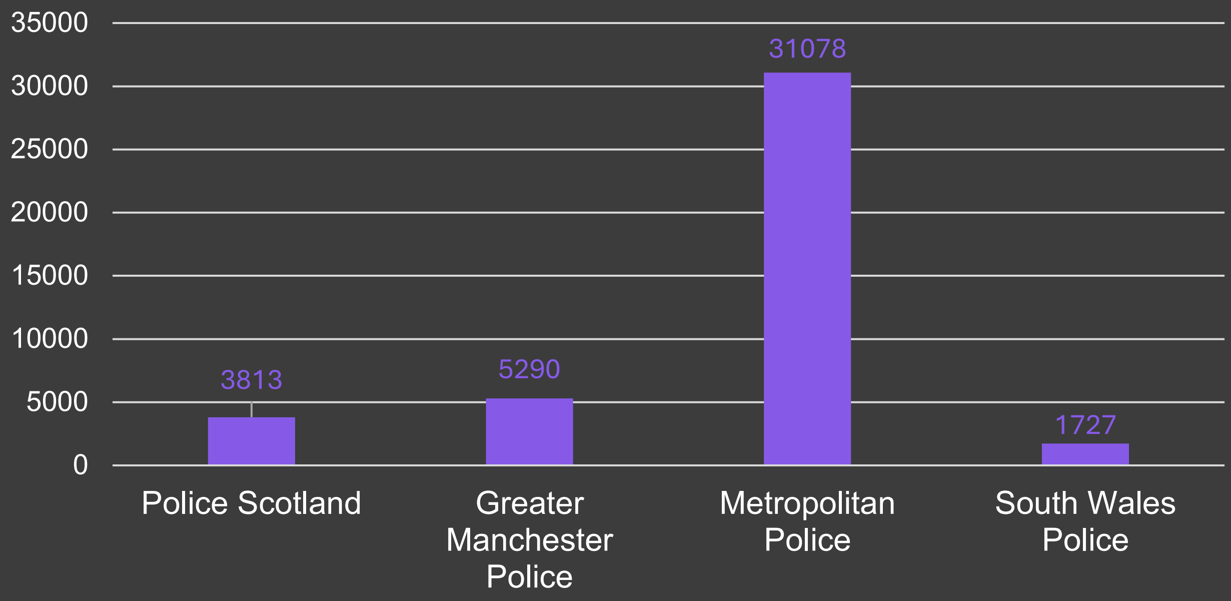
There were 3813 probe images (recovered from e.g. CCTV or crime scenes) searched against PND facial searches, and 193 probe images searched against CAID facial searches for 2023-24.

Data volumes of facial searches (April to March)



Comparative data volumes across UK related to PND facial searches[1]

Total PND facial searches for 2023/24



[1] UK Home Office, statistics received directly from the Home Office to SBC in December 2024.

Key findings

Throughout this report we use the generic term retrospective image search technologies as a collective term to describe use of the facial search functionality within the UK Police National Database (PND) and use of the facial matching function within the UK Child Abuse Image Database (CAID) by Police Scotland. In discussions relative to PND and CAID we also use the relevant search or matching descriptor, but in essence the terminology is interchangeable.

Lawfulness

The use of retrospective image search technology is both lawful and ethical in Scotland. While there is no specific primary legislation in Scotland or the UK governing the use of facial image search, the police in Scotland have been manually comparing images captured at crime scenes to images of previously arrested people for as long as photography has existed and for at least 120 years. Retrospective image search seeks to make this manual process (which is still in existence) more effective and far less labour intensive by producing a shortlist of 'potential' matches for further human investigation. Police Scotland has never deployed or used live facial recognition technology.

It is entirely lawful for Police Scotland to seize evidential materials for the purposes of the investigation, prevention, and detection of crime. The general duties of a constable to prevent and detect crime and protect life and property are made explicit in Section 20 of the Police and Fire Reform Act 2012. Part 3 of the UK Data Protection Act 2018 provides a further explicit legal basis for the processing of personal data for law enforcement purposes including by wholly or partly operated means. The Scottish Biometrics Commissioner's Code of Practice also provides statutory biometric guidance for existing and new technologies within the criminal justice and policing context in Scotland. Accordingly, the Commissioner is satisfied that there is an adequate legal framework in Scotland within which the police may use retrospective image search technologies.

Effectiveness

The evidence indicates that retrospective image search has limited use in practice, and it is of limited overall effectiveness to policing. Approximately 98% of searches conducted by Police Scotland fail to produce any potential matches. This suggests that the technology's current application may not be delivering significant operational value in the majority of cases.[2]

[2] Total number of RIS = Total number of PND Facial Searches (3813) + Total number of CAID Facial Searches (193) = 4006. Evidence of positive matches Total = PND positive matches/leads (57) + CAID positive matches or media verifications (24) = 81. Positive match rate total = evidence of positive matches total (81) / total searches (4006) = 2.02% positive matches. Hence there is almost 98% of searches which produce no match/intelligence lead.

CAID facial matching has made some contribution to improving the effectiveness of investigations into online child sexual abuse and exploitation crimes and ensuring staff and officers' wellbeing working in this area.

Policy development on retrospective image search

No specific Police Scotland policy exists for retrospective image search technology. Police Scotland personnel are aware of relevant technical guidance by the Home Office. Police Scotland aims to adopt a comprehensive Biometrics Policy document, incorporating the use of retrospective image search technologies by 31 October 2025.

Understanding and training on ethical considerations

Police Scotland's officers and staff demonstrate a strong understanding of fairness, integrity, respect, and human rights. Existing training focuses on the technical process of the technology. Enhanced training focused on ethical considerations, technological risks, and legal and policy developments is necessary to equip officers to address the complex and novel challenges associated with retrospective image search technology.

Data volumes

The total volumes of retrospective image searches conducted on PND and CAID by Police Scotland was 4006 for 2023-24. The vast majority of crimes reported to the police in Scotland do not have an image obtained during the enquiry investigation meaning that, quantitatively, they do not play a statistically significant role in most police investigations, although it can have a high qualitative value when dealing with some serious crime types. This has been exemplified in sanitised case studies below.

Algorithmic reliability

Current algorithmic use for PND and CAID image searches within the systems provided to all UK police forces by the Home Office are not accredited to any international scientific or forensic accreditation standard. Police Scotland should always exercise due diligence before deploying any biometric enabled technology in Scotland to ensure that the scientific limitations of any matching capabilities, and consequentially the operational risks associated with their use are properly understood, including to ensure compliance with the Scottish Biometrics Commissioners Code of Practice.

Technological limitations

Current limitations in retrospective image search technology, includes issues related to accuracy, dependency on Home Office decisions, low-quality images on the Police Scotland Criminal History System (CHS) which reduce the functionality's effectiveness for system searches. This gap could mean that people who have had their custody image previously taken and recorded in CHS, are not being detected on PND searches. It would be important to address those to better inform future decision in the adoption of new products and technology, including participation in the UK Home Office strategic facial matching project.

Human oversight in decision-making

Decisions involving retrospective image search in Scotland always involve human verification, ensuring accountability and oversight in the PND and CAID processes.

Data collection, evaluation and transparency

Police Scotland does not currently collect, store, or analyse specific data to assess the effectiveness of retrospective image search technology. Despite this, staff interviewed expressed a consensus on the utility of retrospective image search in criminal investigations, particularly in combating child abuse, reducing workloads, and supporting officer welfare.

Police Scotland does not publish management information pointing to the effectiveness of the retrospective image search functionality within PND or CAID. The absence of any published evaluation makes it difficult for the public to understand whether these are effective policing tools.

PND processing of images

The PND contains significant volumes of images of innocent individuals from England and Wales, including children, victims, witnesses, and vulnerable persons. Police Scotland mitigates this risk by removing Scottish images of individuals who were arrested but not subsequently convicted. However, in the case of an individual who has other previous convictions, the image taken would not be removed and the most current image obtained will be retained.

AI-generated content challenges

The proliferation of AI-generated or synthetic images depicting child sexual abuse presents a growing challenge for policing. Police Scotland's Data Science Strategy references the use of artificial intelligence in the commission of crime and emphasises the need of policy and partnerships to combat the challenges of AI enabled crime. However, Police Scotland has not produced specific guidelines for officers and staff on this issue.

SBC complaints

During the 2023 -24 financial year and up to the date of completing our fieldwork in January 2025, no complaints from members of the public have been received by Police Scotland in relation to the use of retrospective image search and no complaints have been received by the Biometrics Commissioner pertaining to the use of such technologies.

Summary of recommendations

Recommendation 1

Police Scotland should develop a bespoke policy on the use of retrospective image search technologies including those used within the UK Police National Database (PND) and the UK Child Abuse Image Database (CAID). The new policy should include specific guidance on scope, legal and ethical use, data collection and retention periods, prohibited uses, accuracy, reporting and oversight, training, community engagement and complaints. This policy should be developed and consulted with all key stakeholders.

Recommendation 2

Police Scotland should note the limited effectiveness of existing retrospective image search technologies provided to UK policing by the Home Office and related concerns about the quality and resolution of Scottish images on the Police Scotland Criminal History System. Police Scotland should then improve the resolution of its custody images before participating in the UK Home Office Strategic Facial Matching Project delivering infrastructure, software services, data migration, and a new and significantly improved UK facial matching service for law enforcement purposes.

Recommendation 3

Police Scotland should conduct a training needs analysis for officers and staff regularly working with retrospective image search technologies in PND and CAID. Such training may be role specific, but as a minimum should ensure that all relevant personnel are made aware of the provisions of relevant UK and Scottish legal frameworks for biometrics and law enforcement including the Scottish Biometrics Commissioner Act 2020, and the statutory Code of Practice approved by Parliament in November 2022. This with a view to ensuring that all staff working with biometric data and technologies have an awareness of relevant legal frameworks and ethical considerations and technological risks.

Recommendation 4

Police Scotland should improve the collection of management information and analysing data to evaluate the effectiveness and efficiency of retrospective image search technologies. Police Scotland should then determine what information it could safely place in the public domain to improve the public understanding of its value.

Chapter 1. Introduction to our assurance review

This report provides a comprehensive review of key issues related to retrospective image search. It outlines from the opening the key facts, key findings, and recommendations. Chapter 1 introduces the scope and objectives of the review. Chapter 2 defines essential terms discussed in the report. Chapter 3 examines relevant law and policy, providing the legal and policy framework for our analysis. Chapter 4 details the evidence-gathering process and findings, including data volumes and anonymised sanitised cases to illustrate value. Finally, Chapter 5 discusses the future legal and ethical challenges which should be considered by Police Scotland. This report aims to provide clear insights and actionable recommendations to support informed decision-making in the use of this biometric technology by Police Scotland.

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 updated in February 2023. The specific methodology for this review was outlined in a terms of reference agreed between partners, which was published on the Commissioner's website.

About the 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)
- Scottish Police Authority (SPA)
- 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.

Our values

As a values-led organisation, we will conduct our activities in a way that is Independent, Transparent, Proportionate and Accountable.

Independent

We will always act independently and publish impartial and objective review reports. Our professional advice will be informed and unbiased. The Scottish Biometrics Commissioner is a juristic person, appointed by the Monarch on the nomination of the Scottish Parliament and is independent of Scottish Government.

Transparent

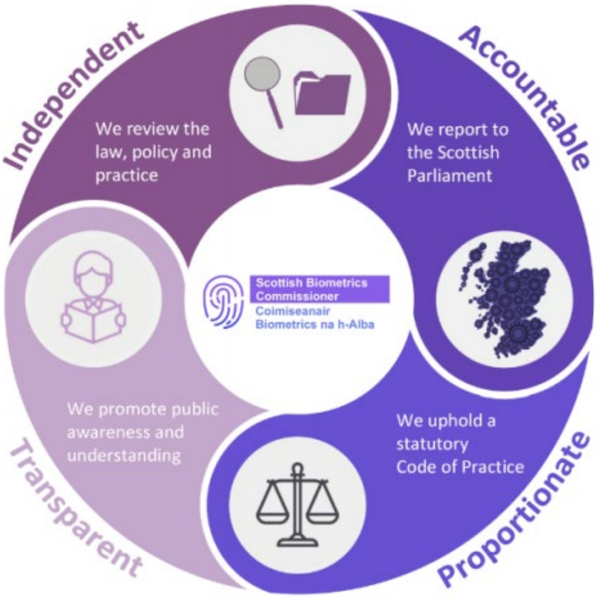
We will be open about what we do and give reasons for our decisions. We will publish our reports and findings and will not restrict information unless deemed necessary to protect the identity of data subjects, or due to wider public interest considerations. For example, section 19 of the Scottish Biometrics Commissioner Act 2020 provides that the Commissioner or a member of staff must not knowingly disclose confidential information unless necessary in the exercise of the Commissioner's functions. This means that we will never publish sensitive or specific case information in circumstances that could compromise police investigations or hand competitive advantage to criminals.

Proportionate

We will ensure that our activity is proportionate and does not exceed what is necessary to achieve our statutory purpose. We will minimise the burden of any review activity on Police Scotland, the Scottish Police Authority, and the Police Investigations and Review Commissioner. We will ensure that the way that we do what we do is necessary, effective, and efficient.

Accountable

We will be accountable for what we do to the Scottish Parliament and will submit ourselves to whatever scrutiny is appropriate to our function. We will promote equality, diversity, and human rights in everything that we do.


Independent
We review the law, policy and practice
Accountable
We report to the Scottish Parliament
Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba
We promote public awareness and understanding
Transparent
We uphold a statutory Code of Practice
Proportionate

Our power to work with others

Section 3 of the Scottish Biometrics Commissioner Act 2020 confers a power on the Commissioner in the exercise of his functions to work, assist and consult with other named bodies. This includes amongst others, Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner. This Assurance Review is conducted by the Scottish Biometrics Commissioner working in partnership with HM Inspectorate of Constabulary Scotland (HMICS). HMICS assisted the review by identifying and assessing the effectiveness of the retrospective facial searching tools used by the Police in terms of producing actionable intelligence leads.

About HMICS

His Majesty's Chief Inspector of Constabulary in Scotland (HMICS) provides independent scrutiny of both Police Scotland and the Scottish Police Authority (SPA). Its approach is to support Police Scotland and the SPA to deliver services that are high quality, continually improving, effective and responsive to local needs.

In looking at retrospective image search technologies, this assurance review focuses primarily on how those biometric enabled technologies are used by Police Scotland in relation to the automated searching of images. We use retrospective image search as a generic term in this report. This includes images derived from crime scenes and related policing enquiries searched against the UK Police National Database (PND), and regarding child protection matters the UK Child Abuse Image Database (CAID) to assess how effective (or not) those technologies are.

Aims

The strategic aim of this joint review is to provide assurance to the Scottish Parliament that the retrospective image search tools currently being used by Police Scotland are lawful, effective, and ethical. In particular, the emphasis of the review will be on effectiveness and explicitly:

"To assess the effectiveness of the retrospective facial searching tools used by Police Scotland in both PND and CAID in terms of producing actionable intelligence leads, and to consider what management information is held by Police Scotland pointing to their overall effectiveness"

Methodology and scope

Several qualitative and quantitative methods were used to answer the key aims of this review. A further detail of the methodology for evidence gathering can be found in Chapter 5 of this report. The methodology for this review includes (but not be limited to):

- The volumes of retrospective searches being conducted on PND by Police Scotland in the most recent calendar or fiscal year
- The volumes of retrospective searches being conducted on CAID by Police Scotland in the most recent calendar or fiscal year
- An audit of the PND reason codes via the Police Scotland PND Bureau for such searches to ensure lawful basis

- Any management information pointing towards their effectiveness in producing actionable intelligence leads
- Identifying any matters pertinent to the quality of probe or gallery images uploaded to PND and CAID by Police Scotland
- Considering what steps have been taken by Police Scotland to ensure that ethical considerations form part of the relevant Standard Operating Procedures for conducting retrospective facial searches on PND and CAID, including any due diligence steps taken by Police Scotland to ensure that the Home Office algorithms are free from bias and discrimination
- Gathering any sanitised case studies pointing to the value of retrospective image search in contributing towards solving serious crimes, or in protecting children from abuse
- Ascertaining whether Police Scotland (other than in circumstances within the remit of the Investigatory Powers Commissioner) has requested any retrospective image searching on third-party databases such as the UK passport image database
- Identifying ethical and other considerations associated with any future decision by Police Scotland to adopt the Home Office Strategic Facial Matcher product.

The legal and policy standards considered for this review included the SBC Code of Practice, police guidance such as SOP and the SBC National Assessment Framework for biometric data outcomes, which ensures a consistent and objective approach to our work.

Our National Assessment Framework considers six overarching themes, namely:

- Leadership and governance
- Planning and process
- People
- Resources
- Partnerships
- Outcomes

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

The scope of this assurance review extends to:

- Police Scotland

The review focuses solely on questions relating the lawful, effective, and ethical use of biometric data in Scotland by Police Scotland. Accordingly, there will be no wider assessment of the non-biometric data elements of either PND or CAID. The review is restricted to use by Police Scotland and to the remit of the Scottish Biometrics Commissioner and His Majesty's Inspectorate of Constabulary in Scotland. Accordingly, there was a minimum engagement with the Home Office and National Crime Agency where Police Scotland had reliance on policy documentation for PND and CAID, or for qualitative assessment of International Cooperation on use of CAID. The review did not consider biometrics used in covert policing activity or matters within the statutory remit of the Investigatory Powers Commissioner's Office (IPCO).

This assurance review provides four recommendations to Police Scotland. My expectation as Commissioner is that any recommendations from our assurance reviews will result in an action plan by the organisation(s) to whom they are directed and taken forward to enable relevant good practice to be disseminated across Scotland to promote continuous improvement. I will monitor actions to address any recommendations made and will report on progress and outcomes in my Annual Report to the Scottish Parliament. Where a recommendation is made to Police Scotland, the SPA will also monitor progress through normal mechanisms for holding the Chief Constable to account.

I wish to extend my thanks and appreciation to Police Scotland for facilitating our assurance activity and information requests, including Gillian Jones, Head of Biometrics and Diana Dundas, Biometrics Data Lead and to the many and immensely helpful officers and staff from Police Scotland who facilitated our field visits.

Our joint assurance review was led and produced by Diego Quiroz, SBC Operations Manager assisted by Gavin Phillip HMICS Associate Inspector and Ross Macdonald, SBC Director.

Dr Brian Plastow
Scottish Biometrics Commissioner
March 2025

Chapter 2. 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.

Image search system

An image search system is a technology that enables trained and authorised users to search an image of interest such as a crime scene image against a database containing images of persons previously arrested by the police or, in the case of child protection, illegal images of victims, offenders and offending often posted on the dark web. This type of search is often used in various fields, including digital forensics, medical imaging, and media. The process typically involves using metadata, tags, or advanced image recognition algorithms to locate relevant images within a large dataset. Depending on the system algorithms can identify either faces or objects from images.

Retrospective image search

Police Scotland has never deployed live facial recognition technology in Scotland and only uses retrospective image search technology (RIST) via a facial matching or a search functionality. RIST compares static images normally obtained from crime scenes against stored databases containing images of offenders and in some cases victims of crime. Unlike real-time image search, which involves analysing and retrieving images as they are being captured or uploaded, retrospective image search focuses on querying existing archives of images. RIST is an integrated solution and is only used on case-by-case basis when there is a requirement to further research a particular face. RIST is the focus of our assurance review, and it is used to describe **both facial search and matching** functionality in this report.

Except for reserved matters such as counterterrorism investigations, there arere 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. PND gallery is based on custody images from UK police forces and CAID gallery is based on suspects of indecent images of children from previous enquiries which are kept, to be checked against future probe images. In each case, the facial matching software will return a list of potential matches for further human investigation.

Algorithms used to process facial data vary according to the technology provider.[3] The accuracy and positive performance of any facial search system is also dependent on the quality of enrolment images. It is worth noting that unlike DNA and fingerprints (and noting that identical twins share identical DNA but not fingerprints) human faces do not have characteristics of uniqueness. Instead, they have characteristics of similarity and are not on their own unique enough for policing to establish identity to a forensic standard suitable for a court of law.

PND

It is a UK policing national information and intelligence sharing system that enables the police service and a number of other law enforcement agencies to share, access and search locally held information on a national basis, overcoming artificial geographical and jurisdictional boundaries.[4] PND is owned by the Home Office. PND was rolled out to UK police forces in April 2011 and was also adopted by the eight legacy police forces in Scotland and the former Scottish Crime and Drugs Enforcement Agency (SCDEA) in April 2011. Prior to the establishment of Police Scotland in 2013, the former Association of Chief Police Officers in Scotland (ACPOS) had already approved the adoption of additional modules for PND including PND Facial Search. 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 PND.

PND has a facial search functionality. This entails a still image of a suspect, known as the probe image, being uploaded to PND, and thereafter being compared with all custody images uploaded to PND from UK forces. Images from suspects come from various sources, including CCTV, Ring Doorbells, fraudulent documents. The probe image used to search against the PND Facial Search gallery can be any one of the following file formats .jpg, .thm, .bmp and .png. The probe image is ideally forward-facing shot of the person to search for and should be no greater than 500KB in size. The results displayed will show matching groups that contain images that matched against the probe image, up to a maximum of 50 results.[5] The quality of the image is a key factor for the effectiveness of the system. PND search functionality has been used in Scotland since 2014.

[3] For example, PND uses Cognitec's FaceVACS technology, Cognitec Systems GmbH.
[4] PND Search User Guide, Version number 9.0 (07 January 2023). College of Policing.
[5] PND Search User Guide, Version number 9.0 (07 January 2023). College of Policing.

When a probe image from a crime scene or incident is uploaded to PND, the algorithm compares facial vectors such as the distance between the eyes, and distance from eyes to the tip of the nose to images derived from previous custody episodes which appear mathematically similar to the software. Although the shortlisted images may be mathematically similar in terms of facial vectors, the potential matches suggested by the software sometimes bear no resemblance whatsoever when examined by the human eye. For example, in the case of a probe image of an older white skinned bald man, the software may suggest a match with a young black skinned woman with a full head of hair. This is because mathematically the facial vectors may be very similar or even identical, whereas to the human eye, one is obviously an older bald white man and the other obviously a younger black woman with a full head of hair. Therefore, the PND facial search functionality is simply intended as a shortlisting tool to assist human decision-making and is incapable of true facial recognition.

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 by the COPFS.[6]

CAID

It is a UK policing secure database of illegal images and videos of children to aid UK law enforcement to identify victims and perpetrators of online child sexual exploitation. When a device is seized under warrant, the examination of it is undertaken by Cybercrime Investigations and Digital Forensics. When potential victims are identified, images are tagged and referred to the Victim ID Unit for further investigation and/or identification. This process enables the creation of safeguarding packages in coordination with the National Crime Agency ensuring victim protection. CAID is owned by the Home Office, managed by West Yorkshire Police, and operated by UK law enforcement agencies.

The CAID database uses facial recognition software[7] by utilising algorithms that convert 2D images into “3D head” images which enables the technology to match a subject’s face from other stored images on the CAID database. Image data is sourced from files extracted from devices legitimately seized from victims and suspects, during an investigation. CAID works by bringing together all the images that the police and National Crime Agency encounter, then the police use the images’ unique identifiers – called hashes - and metadata to identify a victim and perpetrator. This facial matching functionality is run across all historic cases and is set to run automatically against every new case loaded into CAID. When a face or faces are detected in an image, that image is enrolled into the facial recognition system, to create an ‘entity’. CAID then presents the user what it believes to be the ‘best image’ or entity image that it has found in CAID.

This functionality also helps to limit the volume of disturbing images officers are exposed to or are required to manually review. CAID supports international efforts to remove images from the internet. Positive enquiries images are archived and retained for criminal cases only, in line with Police Scotland retention policy.[8]

Police Scotland have been using CAID since 2015, initially using only object /pattern matching, with facial matching function enabled in July 2023.

[6] Further information on image databases can be found in our previous assurance review on images.
[7] CAID uses NEC’s face recognition technology.
[8] Police Scotland, Records Retention SOP, Version 7.

Chapter 3. Law and policy

This section provides an overview of the legal and policy framework in Scotland in relation to retrospective image search for PND and CAID. This includes both a description and assessment of Police Scotland's internal guidance, governance arrangements and procedures. The next chapter covers practice and cross-verification of information through an analysis of police policy documents and observations on the ground.

The law

Images are the most common type of biometric data used for policing and criminal justice purposes. The police have been manually comparing images captured at crime scenes to images of previously arrested people for as long as photography has existed and for at least 120 years in Scotland. Local authority public safety cameras in the form of CCTV were first introduced in Airdrie in 1992, and subsequent evaluation of its proliferation from the mid 1990s onwards has confirmed that its potential to aid in the identification of offenders significantly reduces crime.[9] It is entirely lawful under common law for Police Scotland to seize evidential materials for the purposes of the investigation, prevention, and detection of crime.[10] Furthermore, the general duties of a constable to prevent and detect crime and protect life and property are made explicit in Section 20 of the Police and Fire Reform Act 2012. Part 3 of the UK Data Protection Act 2018 provides a further explicit legal basis for the processing of personal data for law enforcement purposes including by wholly or partly operated means. The Scottish Biometrics Commissioner's Code of Practice also provides statutory biometric guidance for existing and new technologies within the criminal justice and policing context in Scotland.

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. 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 and Image Assurance Reviews, Independent Advisory Group on the Use of Biometric Data in Scotland in 2018 and a HMICS' Audit and Assurance Review in 2016.[11]

[9] The Airdrie study by the then Scottish Executive reports crime reduced in the CCTV area by 21%.

[10] It is noted that in Catt the European Court of Human Rights expressed concern regarding reliance on the use of common law powers for invasive surveillance measures, in this case the …. The Court did not, however, rule on this point. Catt v. the United Kingdom, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 105.

[11] There are notable exceptions, for example 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. In addition, 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."

There are also a number of soft law documents that cover this technology, including:

- Home Office's PND user guide[12]
- Home Office's Child Abuse Image Database guide[13]
- Police Scotland's Victim Identification Awareness Presentation[14]
- Authorised Professional Practice, Live Facial Recognition, College of Policing [15]

Accordingly, the Commissioner is satisfied that there is an adequate legal framework in Scotland within which the police may use retrospective image search technologies.

The use of retrospective image search technology (RIST) by Police Scotland involves information about an individual's physical characteristics within the meaning of Section 34 of the Scottish Biometrics Commissioner Act 2020. This applies in respect of all facial images captured and analysed by facial search systems. Therefore, the use of such technology must meet the relevant requirements (12 principles) of the SBC Code of Practice. These are:

1. Lawful authority and legal basis
2. Necessity
3. Proportionality
4. Enhance public safety and public good
5. Ethical behaviour
6. Respect for the human rights of individuals and groups
7. Justice and accountability
8. Encourage scientific and technological advancement
9. Protection of children, young people, and vulnerable adults
10. Promoting privacy enhancing technology
11. Promote equality
12. Retention periods authorised by law

[12] PND User Guide V. 9.0, Home Office, available at Police Scotland's intranet.
[13] Child Abuse Image Database guide, January 2019, Version 0.4 (draft).
[14] PowerPoint presentation available at Police Scotland's intranet.
[15] Available at https://www.college.police.uk/app/live-facial-recognition.

Police Scotland policy and practice

The review conducted a detailed engagement and information request on current policy and practice regarding PND and CAID. There are a number of processes that support decision making for the use of RIST by Police Scotland, including:

Impact assessments

- **Data Protection Impact Assessment (DPIA)**
  A DPIA is a process designed to help Police Scotland systematically analyse, identify, and minimise the data protection risks of a project or plan. It is a key part of accountability obligations under the UK GDPR. It also helps to assess and demonstrate compliance with all the organisation's data protection obligations and SBC Code of Practice.

- **Equality and Human Rights Impact Assessment (EQHRIA)**
  EQHRIA are an important mechanism for enabling equality and human rights considerations to be embedded into the policies, practices, procedures of this technology. It also ensures compliance with human rights obligations and SBC Code of Practice.

- **Data Ethics Assessment (DEA)**
  DEA are part of the Data Ethics Framework; their aim is to ensure that the organisation has the appropriate mechanisms to identify and address ethical challenges in relation to data and data driven technology. CAID was subject thereafter to an Independent Ethics Advisory Panel (IEAP) to ensure ethical considerations of the use of the facial matching technology.

The rights based pathway

Police Scotland and the Scottish Police Authority have introduced a new internal procedure to support decision making and to maintain public trust and confidence in the organisation in respect of the adoption and use of technology. The express need for this approach was borne out of the lessons learned from Police Scotland's initial introduction of Digital Triage Devices in 2020. This commitment is reflected in a number of technology strategies and adopted from the Emerging Technologies Independent Advisory Group (ETIAG) recommendations. Police Scotland and Scottish Police Authority has developed a Memorandum of Understanding (MOU) for the purpose of self-assessing the adoption of new technologies.[16] The Rights Based Pathway has not been applied retrospectively to old technologies such as PND facial search.

There has been extensive engagement and support internally and externally throughout the development of this process and in keeping with Police Scotland's Values of Fairness, Integrity, Respect and Human Rights.

[16] SPA, Policing in a Digital World Programme, 15 June 2023.

PND governance

PND is a UK policing information and intelligence sharing system, which was rolled out to UK police forces in April 2011 and was also adopted by the eight legacy police forces in Scotland and the former Scottish Crime and Drugs Enforcement Agency (SCDEA) in April 2011. Prior to the establishment of Police Scotland in 2013, the former Association of Chief Police Officers in Scotland (ACPOS) had already approved the adoption of additional modules for PND including PND facial search. The PND facial search module was introduced in 2014.[17]

There are 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. PND has a high number of duplicate images as the police often hold multiple images of the same person. It is unknown exactly how many nominals are within PND. Furthermore, PND contains high volumes of images of innocent people from England & Wales despite the 2012 ruling by the High Court in England that this was unlawful.[18] This means that PND contains hundreds of thousands of images of people that are being illegally retained. This issue has been amply discussed in other reports[19] and by courts, including by the European Court of Human Rights (ECtHR). In turn, this means that Police Scotland also has access to the images of persons from England and Wales which should not be retained on PND.

Considering the UK' slow compliance with the Gaughran vs UK judgment (2020),[20] the Department for the Execution of Judgements of the ECtHR established an enhanced procedure for its implementation, which is ongoing. The adoption of the necessary execution measures is supervised by the Committee of Ministers of the Council of Europe - made up of representatives of the governments of the 46 member states - assisted by the Department for the Execution of Judgments of the Court. On 28 November 2024, the UK submitted an updated action plan, which is currently under review.

It is also important to note that last year, 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.[21] The NPCC has now established a national programme to ensure a legally complaint retention regime.

There is no specific Police Scotland policy related to PND retrospective facial search (RFS). A Biometrics Policy is due to be published early 2025 to include overarching section on RFS. Vulnerable people and children's data is not specifically regulated at present.

[17] A full explanation of facial matching functionality of PND can be found in Chapter 2.
[18] [2012] EWHC 1681 (Admin).
[19] HMICS Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND).
[20] This case concerns the indefinite retention of personal data taken from the applicant in 2008 in connection with his spent conviction in Northern Ireland for a minor offence. The judgment requires a revision of the current framework governing the retention of biometric data and photographs for both convicted and non-convicted persons with adequate safeguards in line with the S, and Marper and Gaughran cases.
[21] For further discussion on this issue, see: SBC Assurance Review on Images.

PND RFS was introduced prior to implementation of Data Ethics and Rights Based Pathway.

Police Scotland is represented on NPCC Facial Recognition Board and PND Regional Users Group. PND users can access guidance, shared knowledge, and national contact via the UK Knowledge Hub.

Strategic Governance of biometric data by Police Scotland is exercised through a Biometrics Oversight Board chaired by the Assistant Chief Constable Major Crime. The Scottish Biometrics Commissioner attends this Board in an advisory capacity.

Algorithms

The US National Institute of Standards and Technology (NIST) has conducted tests to quantify demographic differences in contemporary face recognition algorithms. NIST is the leading face recognition independent evaluator. The PND developer (Cognitec) is one of vendors assessed in 2019, which is the most up-to-date available report. NIST report provides details about the recognition process, notes where demographic effects could occur, details specific performance metrics and analysis, gives empirical results, and recommends research into the mitigation of performance deficiencies.

NIST found that modern facial recognition algorithms show varying levels of demographic bias. False positives (incorrect matches) are significantly more affected by demographics than false negatives (missed matches), with rates differing by factors of 10 to over 100 across groups.[22] With high-quality images, false positives are highest for West and East African and East Asian individuals and lowest for Eastern Europeans. Women also experience more false positives than men, though racial disparities are more pronounced. False negatives are highest for Asian and American Indian individuals, while white and African American individuals have the lowest rates.

However, with lower-quality border crossing images (e.g. passport control points), false negatives are more frequent for people from Africa and the Caribbean, particularly older individuals. These variations highlight the impact of image quality on algorithm performance.

[22] A false positive means that the software wrongly considered photos of two different individuals to show the same person, while a false negative means the software failed to match two photos that, in fact, do show the same person.

The algorithm used in PND ranked 20th out of 203 algorithms tested from 51 commercial developers in 2019. We note that the algorithm was upgraded from Cognitec FaceVacs Version 5.1 (which uses comparison algorithm B10) to FaceVACS-DBScan ID 5.5.0 (which uses B12) in November 2021. The Home Office conducted their own testing and the NPCC conducted Equality testing between the old and new algorithm used for facial searching against data sets including on ethnicity and gender. Algorithms used in PND are not accredited to any forensic ISO standard, this means that any potential matches could not be relied upon to a standard suitable for presentation to the courts as evidence.

The implications of NIST results mean that it is crucial for the system owner to know their algorithm. This includes measuring accuracy of the operational algorithm and testing images of individuals in various demographics and national contexts to improve future performance and response to the specific needs of the region. It is important to regularly audit the data for biases that could skew the algorithm's performance or outcomes in the local context. As most systems are configured with a fixed threshold, it is necessary to report both false negative and false positive rates for each demographic group at that threshold.[23] PND facial search involves humans in the decision-making process.

Users

Authorised PND users can directly use the facial search functionality. Images are uploaded to PND from Police Scotland via the criminal history system (CHS).[24] This functionality allows the user to search against all custody images loaded within PND. There are currently 320 users who can submit individual, triggered and/or bulk facial searches with up to a maximum of 50 images in a single bulk search submission.[25]

Search results are treated as intelligence and should be assessed and developed by an intelligence professional and or the lead investigator. PND facial search results do not provide evidence for a formal identification.

Training

PND users are trained and registered with a validated user ID. There were 320 active users in Police Scotland during our fieldwork in October 2024.

PND training covers facial search, however the use of this functionality is not evaluated. Training does not cover the SBC Act and Code of Practice. Current policy guidance does not extend to key factors such as: the limitations of facial search technology, risks linked with its use (such as automation bias), or how officers can approach the necessity and proportionality test. Such guidance can play a key role in ensuring that officers are equipped to grapple with the complex and novel issues raised by RFS.

[23] National Institute of Standards and Technology Interagency or Internal Report 8280
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8280, 81 pages (December 2019).

[24] CHS contains all records and images of charged and convicted persons in Scotland. Further information on image databases can be found in our previous assurance review on images.

[25] PND Search User Guide, Version number 9.0 (07 January 2023). College of Policing

Effectiveness of RFS

The information provided by Police Scotland suggests that the organisation does not collect, store, or analyse specific data to evaluate how effective the PND facial search system is. The Commissioner has attended the Police Scotland Biometrics Oversight Board since 2021 and no management information on the use of the facial search functionality within PND has been tabled for discussion in the past 4 years. There is extraordinarily little data and insights collected systematically to help monitor performance, identify issues, and inform decision-making.

For example:

- How many identifications from the system lead to successful outcomes (like arrests or resolved cases)?
- How accurate are the matches made by the facial search system?
- What are the rates of false positives and negatives?

It is important to note that in the absence of such data, it is not possible to assess the reliability, effectiveness, and fairness of PND RFS.

The quality and resolution of images can significantly impact the effectiveness of retrospective facial searches. We were informed about the insufficient quality and resolution of Scottish images on the Police Scotland Criminal History System (CHS). This affects a portion of custody images captures between 2019-2024 meaning that a sizeable portion of custody images are not searchable under PND facial search functionality. This gap could mean that people who have had their custody image previously taken, are not being detected on future probe images uploaded by Police Scotland, which could lead to crimes not being detected.

We were informed that a software issue causing custody images obtained at the point of capture, are lower than the recommended minimum size (20kb), and combining this with additional compression techniques, it has made them unsuitable for use within the PND for facial searching purposes. Extreme caution must be exercised with any retrospective ICT fix to uncompress these images. If they cannot be fully restored to their original format, the reliability of the data could be significantly compromised. It is our assessment that Police Scotland should ensure this issue is solved, particularly considering the adoption of new systems such as the UK Home Office Strategic Facial Matching Project.[26]

Retention

In terms of retention policies, unsuccessful match is weeded within 48 hours (probe image). Successful match is stored with case data and retained in accordance with relevant retention policy and schedule.[27]

An additional risk emerges in using PND facial search functionality as PND contains high volumes of images of innocent people from England & Wales despite the 2012 ruling by the High Court in England that this was unlawful.[28] Police Scotland removes images of persons arrested and not subsequently convicted (and who have no previous conviction) from CHS and PND as soon as possible and in accordance with the SBC Code of Practice.

Internal accountability

PND is audited by Police Scotland. Audit logs will record sufficient information about each transaction to enable identification of individuals (both PND users and the subjects of PND records), making the audit logs subject to regulatory and legislative controls. However, during our review we discovered that Police Scotland conducts no audits of the use of retrospective facial search and has conducted no post-implementation review of its effectiveness. This points to weaknesses in Police Scotland's strategic governance over biometric data and technologies including the absence of any documented strategy or plan setting out the Police Scotland 3-, 5-, or 10-year vision. Not conducting evaluation, and not having a strategy makes it difficult for Police Scotland to know which technologies it should use (or not use) and which it should invest in (or not invest in). We have made similar observations in our DNA Assurance Review laid before the Scottish Parliament in February 2025.

[26] The Strategic Facial Matching Project aims to establish a national facial matching service for law enforcement purposes, with initial developments focused on retrospective facial recognition. This project will entail infrastructure, software services, and data migration.

[27] Police Scotland, Records Retention SOP, Version 7 or current year + 6 for general crime, Current year + 12 for serious crime.

[28] [2012] EWHC 1681 (Admin).

CAID governance

CAID is a secure database of illegal images and videos of children to aid UK law enforcement to identify victims and perpetrators of online child sexual exploitation. The CAID database uses Facial Recognition Technology (FRT) by utilising algorithms that convert 2D images into "3D head" images which enables the technology to match a subject's face from other stored images on the CAID database. The total number of images in CAID is 35 million of which 1.6 million are video. Police Scotland have been using CAID since 2015,[29] initially using only object/pattern matching, with facial matching function enabled in July 2023.

CAID facial matching functionality has undertaken several layers of internal approval. Cybercrime Policing in a Digital World Programme (PDWP) completed various documents in relation to the use of CAID and CAID FM which extended to the Data Protection Impact Assessment (DPIA), Equality and Human Rights Impact Assessment (EqHRIA) and an early iteration of the Data Ethics Assessment with Data Ethics. The Programme thereafter instigated an Independent Ethics Advisory Panel (IEAP) to ensure consideration of the ethical aspect of the use of the FM technology within CAID in 2022. The Panel was supportive of Police Scotland introducing this technology to both improve effectiveness in investigating online child sexual abuse and exploitation crimes and staff and officers' wellbeing working in this area. In April 2023, CAID facial matching was reviewed and approved by the Senior Leadership Board. CAID facial matching was also used as a proof of concept for the Rights Based Pathway.

There is no specific Police Scotland policy related for the deployment of any FRT and facial matching on CAID. A Biometrics Policy is due to be published early 2025 to include overarching section on RIST. CAID Programme Board is held quarterly and chaired by the Home Office Senior Responsible Officer (SRO). The agenda is on product delivery, procurement, benefits, and deployment. The Programme Board is collaborative rather than prescriptive, so data is held under a Joint Controllers Agreement (JCA) so each Chief Constable can act and use CAID in a manner which matches their business need.

Images uploaded by Police Scotland may be shared with other forces in UK, National Crime Agency and the Crown Office and Procurator Fiscal Service (COPFS). In addition, the Internet Watch Foundation (IWF) assists law enforcement by removal of harmful content and images (known hashes) that are identified by CAID, and their removal from the internet.

[29] A full description of CAID facial matching technology can be found in chapter 3.

Algorithms

Like PND, CAID face recognition algorithms were assessed by NIST. The 2019 NIST report provides details about the recognition process, notes where demographic effects could occur, details specific performance metrics and analyses, gives empirical results, and recommends research into the mitigation of performance deficiencies. The implications of NIST results mean that it is crucial for the system owner to know their algorithm. This includes measure accuracy of the operational algorithm and testing images of individuals in various demographics and national contexts to improve future performance. As most systems are configured with a fixed threshold, it is necessary to report both false negative and false positive rates for each demographic group at that threshold.[30] Algorithm used in CAID is 6th ranked out of 279 algorithms for frontal mugshot identification. CAID facial search involves humans in the decision-making process. Algorithms used in CAID are not accredited to any forensic ISO standard.

Users

Limited staff have the access to conduct a facial search over the CAID environment. There are 12 CAID users across Scotland. CAID is only employed to help identify both victims and perpetrators of abuse. Police Scotland uses a cached local version and runs regular uploads/updates to retain up to date library access. Digital Forensics can access the version of CAID used internally to filter and categorise images, via Griffeye software.

Image data is sourced from files extracted from devices legitimately seized from victims and suspects, during an investigation. No data used in facial matching is sourced from external sources. To protect personal data, generic labels are used instead of personal details when referring to the case, ensuring the victim's information remains confidential.

Training

CAID training is provided by Home Office via train the trainer course to nominated Police Scotland staff. Trainers thereafter provide training to other Police Scotland colleagues. Training covers facial matching; however, this is not evaluated. Training does not cover the SBC Act and Code of Practice.

Current policy guidance does not extend to key factors such as: the limitations of facial search technology, risks linked with its use (such as automation bias), or how officers can approach the necessity and proportionality test. Such guidance can play a key role in ensuring that officers are equipped to grapple with the complex and novel issues raised by facial matching.

[30] National Institute of Standards and Technology Interagency or Internal Report 8280
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8280, 81 pages (December 2019) available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Efficiency of facial matching

The information provided by Police Scotland suggests that the organisation does not collect, store, or analyse specific data to evaluate how effective the CAID facial matching system is. There is extraordinarily little data and insights collected systematically to help monitor performance, identify issues, and inform decision-making. For example:

- How many identifications from the system lead to successful outcomes (like arrests or resolved cases)?
- How accurate are the matches made by the facial search system?
- What are the rates of false positives and negatives?

It is important to note that in the absence of such data, it is not possible to assess the reliability, effectiveness, and fairness of CAID facial matching.

Retention

In terms of retention practice, positive enquiries images are archived and retained for criminal cases only, in line with Policy Scotland' retention policy [31] (i.e. Production Retention Schedule) and managed by a Data Retention Manager within Cybercrime. No hard copy data is retained. Unidentified child victim images are retained for 99 years. Victims who have facial image voluntarily uploaded to assist with investigation, may request their image removed upon request.

Internal accountability

CAID is audited by the Home Office and Police Scotland. Each instance of CAID is audited by the force accessing it and the central system is audited by a national NPCC auditor. Police Scotland has recently trained an auditor for the CAID system and are actively developing the audit process, which should rectify the lack of audits for retrospective facial matching. Police Scotland has not reviewed CAID effectiveness post-implementation. This highlights weaknesses in its governance of biometric technologies, including the absence of a long-term strategy. As described above, similar issues were noted in our DNA Assurance Review presented to the Scottish Parliament in February 2025.

[31] Records Retention SOP, Police Scotland, Version 7.

Chapter 4. Evidence gathering and findings

This chapter covers evidence gathered during onsite visits to Police Scotland PND Bureau for PND, and the Police Scotland National Child Abuse Investigation Unit (NCAIU) for CAID as well as interviews with the Victim ID unit and regional PND operators. Findings are presented at the end of each section for PND and CAID. This chapter also provides data volumes for retrospective image searches and comparative data with forces in England & Wales. The chapter ends with a number of sanitised case studies pointing to the value of RIST towards solving serious crimes and protecting child abuse.

Methodology

The evidence gathering stage employed a mixed-methods approach combining qualitative interviews and quantitative data analysis. The aim was to assess the effectiveness of retrospective image search technology used by Police Scotland in PND and CAID,[32] both in terms of the SBC Code of Practice and existing legislation. For this we developed a framework based on three objectives:

1. Identify and analyse the policy and types of management information held by Police Scotland,
2. Understand operational challenges and technical limitations, and areas for improvement from the perspective of the staff using the RIST, and
3. Evaluate the effectiveness of RIST to produce actionable intelligence leads.

The review involved two key data collection methods: semi-structured interviews with relevant staff and quantitative analysis of policy, management data, including RIST volume data for 2023-24. A series of interviews and focus groups were conducted between October and December 2024. 17 people participated in this stage. The participants included senior management, trainers, and operators. Interviewees and participants came from the PND Bureau, the Cybercrime Unit, Victim ID covering different geographic locations across Scotland to represent their experience using this technology. We also interviewed representatives from the College of Policing in relation to national training and auditing. A number of key areas of enquiry were presented to the participants in advance for the discussions and interviews. A questionnaire was also sent to internal auditors tailored to improve understanding and effectiveness of the auditing process for PND and CAID. This section summarises those interviews. Limitations to this methodology include, restrictions on accessing all the operational data, bias in self-reporting and technological complexity of RIST systems.

[32] A description of the two systems and databases can be found in Chapter 2.

This methodology outlines a broad approach to evaluate the management and effectiveness of retrospective facial searching tools, including in producing actionable intelligence and the management information Police Scotland uses to assess their utility. This section provides policy and operational insights as well as data-driven evaluations, obtained from the (qualitative) staff interviews and (quantitative) data analysis of relevant documentation.

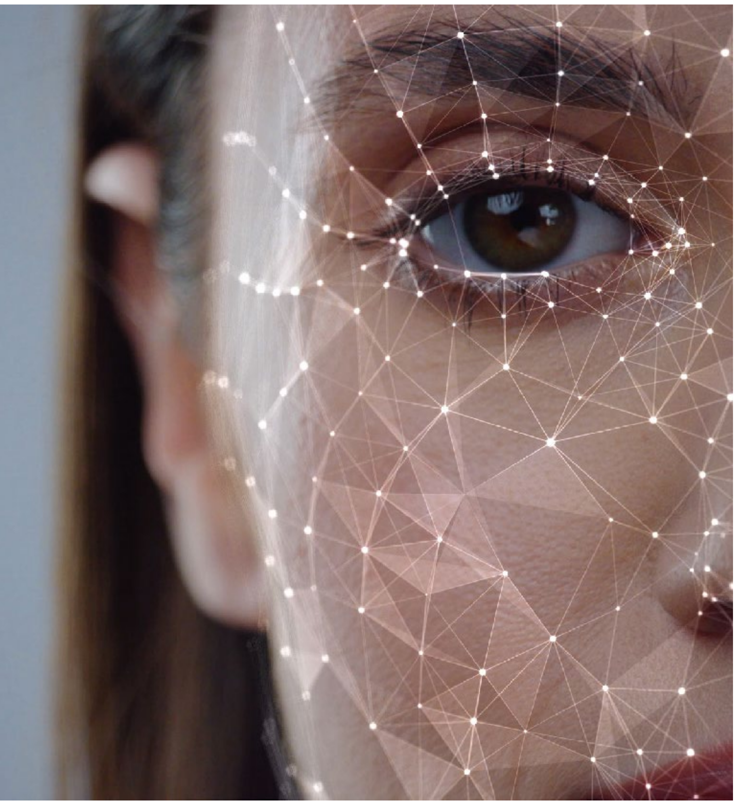
The final themes that emerged from our analysis of the information received are:

- Enhanced policy and procedure around biometric data and system functionality
- Enhanced public oversight
- Improved understanding among officers and staff of how biometric data support the criminal justice system

During our interviews, we were also impressed with the knowledge, professionalism, and dedication to public service amongst the officers and staff of Police Scotland to discharge their duties and protect the public.

Police National Database[33]

Enhanced policy and procedure around biometric data and system functionality. This category includes all findings related to laws, policies, ethical issues, and system requirements.



Request & System Access:

We found that Police Scotland's personnel are cognisant of current technical guidance and procedures to use RIST, including Home Office guidance,[34] even though specific legislation and internal policy for the use of retrospective facial search is lacking. Both senior officers and operators in the PND Bureau and regional offices understand the purpose of the technology, but there is less familiarity with the SBC Code of Practice and Complaints Procedure.

[33] A description of the PND system can be found in Chapter 2.
[34] PND User Guide V. 9.0, Home Office, available at Police Scotland's intranet.

A governance structure for PND users is lacking, despite similar oversight existing in other policing divisions managing biometric data, making it essential to establish consistency. We consider it important to share and ensure consistency as PND bureau is not responsible for divisional users. PND operators are vetted and trained, with a solid grasp of necessity and proportionality principles, but there is uncertainty about whether the required two-day training course adequately addresses biometric data processing risks. Although a form exists to request PND facial search, its purpose and use could be better defined and promoted, as regional variations persist. In most areas, PND facial search requests require supervisor approval, but there is no record of rejected requests, which, if maintained, could improve audits and learning opportunities. Finally, we found that any list of potential matches from a probe image search is subject to human validation to finalise the identification process, ensuring compliance with the SBC Code of Practice. It is worth noting that the effectiveness of PND Facial Search or CAID FM has not been tabled for discussion at any meetings of the Police Scotland Biometrics Oversight Board attended by the Commissioner since 2021.

Data Retention:

Custody images and probe images are retained in accordance with Police Scotland's records retention policy, plus two years for audit purposes. Once the operator logs out of PND the probe image is not accessible to other PND users. However, there is no system in place to identify biometric data that should be deleted in compliance with the SBC Code of Practice and data protection regulations. Additionally, there are no specific guidelines for processing images of children or vulnerable adults, and we observed that the current system does not allow for metadata to be gathered from images. When personal data is shared with other UK public bodies, third-party data sharing agreements are used, but requests from external parties for searches are limited and require supervisor authorisation.

For those reasons, the Commissioner recommends that as part of new Biometrics Standard Operating Procedure currently under development or through a bespoke policy, Police Scotland should include specific guidance on the use of retrospective image search technologies including those used within the UK Police National Database (PND). The new policy should include scope, legal and ethical use, data collection and retention periods, prohibited uses, accuracy, reporting and oversight, training, community engagement and complaints.

Recommendation 1

Police Scotland should develop a bespoke policy on the use of retrospective image search technologies including those used within the UK Police National Database (PND) and the UK Child Abuse Image Database (CAID). The new policy should include specific guidance on scope, legal and ethical use, data collection and retention periods, prohibited uses, accuracy, reporting and oversight, training, community engagement and complaints. This policy should be developed and consulted with all key stakeholders.

PND Facial Search System and Limitations:

We could not obtain information related to due diligence steps taken by Police Scotland to ensure that the Home Office algorithms are free from bias and discrimination. However, NIST provide general face recognition vendor tests, including demographic differences. A further discussion on algorithms bias can be found in chapter 3 of the report.

PND facial search functionality requires operators to invest time in completing the identification process. This includes a strict adherence to image format requirements (JPEG, PNG, BMP, and THM) and a 500kb size limit, which indicates potential technical constraints. We observed that operators extensively use a "snip tool" instead of a dedicated probe image tool. This points to areas for system usability improvement.

We found that a number of Scottish images on the Police Scotland Criminal History System have a low resolution and quality. It is known that algorithms struggle to identify distinguishing characteristics when pixel density is insufficient, especially when the resolution does not capture critical facial regions. Additionally, there is no support for uploading images of distinguishing marks or tattoos, a feature used by other UK police forces. The system also lacks the ability to store unmatched or negative images for future searches, unlike the CAID system, which runs automatically on new cases. We observed that while algorithms assist in suggesting matches via facial similarity scores, operators are instructed to disregard these scores and rely on their own judgment to avoid machine bias. However, no procedures or standards are in place to ensure consistency in this manual process.

Accordingly, the Commissioner recommends that Police Scotland should note the limited effectiveness of existing retrospective image search technologies provided to UK policing by the Home Office and related concerns about the quality and resolution of Scottish images on the Police Scotland Criminal History System. Police Scotland should work on improving the resolution of its custody images before participating in the UK Home Office Strategic Facial Matching Project, aimed to deliver infrastructure, software services, data migration, and a new and significantly improved UK facial matching service for law enforcement purposes.

Recommendation 2

Police Scotland should note the limited effectiveness of existing retrospective image search technologies provided to UK policing by the Home Office and related concerns about the quality and resolution of Scottish images on the Police Scotland Criminal History System. Police Scotland should then improve the resolution of its custody images before participating in the UK Home Office Strategic Facial Matching Project delivering infrastructure, software services, data migration, and a new and significantly improved UK facial matching service for law enforcement purposes.

Enhanced oversight. This section examines issues related to monitoring, transparency, and training.

Audit and Reporting:

PND Bureau operators are highly skilled in using PND facial search due to both their training and experience. While general PND searches are subject to internal audits, there is no feedback mechanism specifically for the facial search function, which complicates the assessment of accountability and effectiveness. Auditors focus on general PND searches, but retrospective facial searches are not audited. Internal auditors undergo regular checks, but there is no evidence of external oversight, including from the Home Office. We were informed that the PND Bureau receives monthly reports on search volumes, but the details of positive or negative matches are not tracked. Additionally, changes in personnel, such as the appointment of a civilian supervisor, suggest operational adjustments, and regular updates with clear documentation of these changes would ensure roles and responsibilities are well-defined and understood by all team members.

Further training:

While there is formal training and assessment for PND that includes facial search functionality, there is no process in place to evaluate the effectiveness of this training in relation to PND facial search. Training availability is also limited by the 340 licences allocated to Police Scotland, with over 80 individuals currently on the waiting list. We encountered that existing training does not cover the Scottish Biometrics Commissioner Act 2020, the Code of Practice, or the amendments to biometric legislation in Scotland.

Current training does not address system biases (e.g. algorithms) or the impact of technology on vulnerable individuals or groups. We were notified that ad-hoc refresher sessions are offered by the Home Office, but developing a formal CPD program, including online training or awareness sessions, could ensure operators stay updated on procedural changes and best practices. It is also important to note that PND users can access guidance, shared knowledge, and national contacts via the UK Knowledge Hub. Notably, participants suggested creating a Scottish PND user group to promote consistent practices, facilitate knowledge sharing, and identify areas for improvement across divisions.

Given this context the Commissioner recommends Police Scotland to conduct a training needs analysis for officers and staff regularly working with image search technologies in PND. Such training may be role specific, but as a minimum should ensure that all relevant personnel are made aware of the provisions of relevant UK and Scottish legal frameworks for biometrics and law enforcement including the Scottish Biometrics Commissioner Act 2020, and the statutory Code of Practice approved by Parliament in November 2022. This with a view to ensuring that all staff working with biometric data and technologies have an awareness of relevant legal frameworks and ethical considerations and technological risks.

We also believe that Police Scotland could appoint a technical lead to oversee algorithm-related concerns of potential biases, to add both to public transparency and effectiveness of the technology. Such a person or group could play a critical role in identifying areas for improvement, standardising approaches, and sharing best practices across divisions.

Recommendation 3

Police Scotland should conduct a training needs analysis for officers and staff regularly working with retrospective image search technologies in PND and CAID. Such training may be role specific, but as a minimum should ensure that all relevant personnel are made aware of the provisions of relevant UK and Scottish legal frameworks for biometrics and law enforcement including the Scottish Biometrics Commissioner Act 2020, and the statutory Code of Practice approved by Parliament in November 2022. This with a view to ensuring that all staff working with biometric data and technologies have an awareness of relevant legal frameworks and ethical considerations and technological risks.

Improved understanding among officers and staff of how biometric data support the criminal justice system. This section examines issues related to effectiveness of RFS to produce actionable intelligence leads.

Efficiency:

According to the information provided by Police Scotland, the organisation does not collect, store, or analyse specific data to assess the effectiveness of PND facial search. While the PND Bureau receives monthly reports on search volumes, there is no tracking of how many identifications lead to successful outcomes, and data on accuracy or false positive/negative rates is not available. Retrospective facial search is currently not audited, and little systematic data is collected to monitor performance, identify issues, or inform decision-making regarding this biometric technology. Tracking these outcomes would offer valuable insights into system efficacy and resource allocation.

Although Police Scotland and SPA Forensic Services produce a quarterly report on Custody Biometrics, which includes the number of PND searches,[35] it could be expanded to include the number of positive matches or intelligence leads, along with sanitised case information, to demonstrate the qualitative value of the technology.

As mentioned before, no management information on PND FS or CAID FM has been presented for discussion during the Police Scotland's Biometrics Oversight Board meetings, which the Commissioner has attended since 2021. We consider that the Biometrics Oversight Board should be the strategic forum to assess the effectiveness and efficiency of RIS technologies.

In this context, the Commissioner recommends Police Scotland to improve the collection of management information and analysing data to evaluate the effectiveness and efficiency of image search technologies.

[35] See for example: https://www.scotland.police.uk/spa-media/j4rpeyug/biometric-custody-data-apr-jun-2024.docx, available at https://www.scotland.police.uk/access-to-information/biometrics/

Recommendation 4

Police Scotland should improve the collection of management information and analysing data to evaluate the effectiveness and efficiency of retrospective image search technologies. Police Scotland should then determine what information it could safely place in the public domain to improve the public understanding of its value.

Child Abuse Image Database[36]

Enhanced policy and procedure around biometric data and system functionality
This category includes all findings related to laws, policies, ethical issues, and system requirements.

Request & System Access:

While there is no specific legislation or internal policy governing the use of retrospective facial matching, personnel interviewed were experts on the technical guidance and procedures for facial matching. CAID follows a victim-centred approach to ensure child victim protection. We also found that senior police officers and operators demonstrate less familiarity with the SBC Code of Practice and Complaints Procedure. It is key to note that facial matching tool is only used on seized devices referred by the cybercrime unit when a child is involved, such as in cases where a device contains suspected indecent images of children (IIOC) and is further referred to Victim ID for identification.[37] Both Victim ID and CAID operators are vetted and trained by the Home Office, and CAID's governance is overseen by the Home Office, which is responsible for data ownership, with governance meetings held every six months, attended by Police Scotland. Interviewed individuals agreed that a specific and inclusive policy would be beneficial for the use of facial matching function in CAID.

[36] This section covers interviews with Victim ID personnel. A description of the CAID system can be found in Chapter 2.
[37] Legal requirements for device seizures under warrants in suspected crimes are established by Cybercrime Investigations and Digital Forensics. An Examination Request Form (ERF) is sent to Cybercrime for examination of seized device. This is assessed by a supervisor ensuring the examination is necessary and proportionate, prior to being processed by Cybercrime to CAID and Victim ID for identification. When potential victims are identified images are tagged and referred to the Victim ID Unit for further investigation/identification. This process enables the creation of safeguarding packages in coordination with the National Crime Agency ensuring victim protection.

Data retention:

During the fieldwork we were informed that positive IIOC images are uploaded to the national CAID library, while non-IIOC images are neither retained nor uploaded, following the principle of minimising unnecessary data retention. To protect victims, personal data within the CAID database is anonymised. Furthermore, physical data is not shared with external partners unless the evidence pertains to another jurisdiction, balancing data security with inter-agency cooperation. Since Scots law does not specify retention periods for images, the current policy aligns with general records retention policy.[38] However, there is no system in place to identify which biometric data should be deleted in compliance with the SBC Code of Practice and data protection laws. We learned that victims have the option to request the deletion of their images from the CAID library in accordance with data protection policy. To ensure data integrity and prevent duplication, all images are assigned unique hash values.

As previously discussed, the policy issues observed in PND were also identified in CAID. Consequently, **Recommendation 1** is applicable to both systems.

CAID Facial Matching System and Limitations:

Like PND, there is no available information on the due diligence steps taken by Police Scotland to ensure that Home Office algorithms are free from bias and discrimination. However, NIST conducts general face recognition vendor tests, including assessments of demographic differences, which are further discussed in Chapter 3 of this report. CAID operates as a closed system using Griffeye software for image extraction and categorisation, with Police Scotland relying on a local version that is periodically updated by West Yorkshire Police. The CAID system allows images to be tagged as “suspect” or “victim,” aiding in systematic categorisation, and uses machine learning to classify images based on pre-existing IIOC categories, though all uncategorised images require human review. We found that this system also offers compatibility scoring for facial models, but staff default to settings that prioritise human verification and professional judgment. A key feature of the system is its limited examination function, which minimises the number of manually reviewed images and reduces staff exposure to traumatic content. Additionally, we were notified that AI-generated IIOC images (which are a criminal offence in Scotland) are increasing significantly. This highlights the need for further guidance on this emerging issue at operational and training positions.

Enhanced oversight. This section examines issues related to monitoring, training, and transparency.

[38] Police Scotland, Records Retention SOP, Version 7.

Audit and reporting:

In our discussions we encountered an elevated level of proficiency on image search technologies. Their training includes a three-day "Train the Trainer" graded national course by the Home Office and a two-day CAID training session. However, refresher training is informal, offered only on an ad-hoc basis without a structured schedule. Facial matching functionality is supervised to ensure accountability in device previews and evidence collection. The system is audited by both Police Scotland and the national CAID auditor at the Home Office, but the absence of feedback mechanisms from these audits makes it difficult to assess accountability and effectiveness.

Further training:

While there is formal training and assessment for the use of facial matching and all operators are fully trained and vetted, there is currently no monitoring of course effectiveness. Similarly to PND operators, CAID and Victim ID are less familiar with Scottish Biometrics Commissioner Act 2020 and the SBC Code of Practice, which changed biometric legislation in Scotland. We also noted that training does not cover system bias (e.g. algorithm, the impact of the technology on vulnerable people /groups and other ethical risks).

There are ad-hoc refresher sessions offered by the Home Office on CAID system, but we think that developing a formal CPD program, including online training or awareness sessions, would help keep operators current on law and policy updates and best practices.

Accordingly, and since the same issues were noted in both PND and CAID, **Recommendation 3** is relevant and applies to CAID.

Improved understanding among officers and staff of how biometric data support the criminal justice system. This section examines issues related to effectiveness of RIST to produce actionable intelligence leads.

Efficiency:

Police Scotland does not collect, store, or analyse specific data to assess the effectiveness of CAID. However, operators and senior management emphasise the system’s value in victim protection, preventing the re-victimisation of children, and improving efficiency. For instance, we were told that a case involving 10,000 images that previously required up to three days to review can now be processed in about an hour using CAID, before final human supervision. It was noted that the cybercrime unit receives monthly reports on search volumes and can produce potential matches, but there is no tracking of how many identifications or positive matches lead to successful outcomes, nor is there data on accuracy or false positive/negative rates.

While both a National CAID Auditor and a Police Scotland Information Security Officer trained in the system conduct audits, there is little systematic data collection to monitor performance, identify issues, or inform decision-making regarding this biometric technology. Police Scotland and SPA Forensic Services produce a quarterly report on Custody Biometrics, which includes the number of PND searches but does not cover CAID facial matching or media verifications.[39] Expanding this report to include the number of children safeguarded from harm, positive matches, intelligence leads, and sanitised case information could help demonstrate the qualitative value of the system.

Since the same issues related to the assessment of effectiveness were identified in both PND and CAID, **Recommendation 4** is relevant and applies to CAID too.

HM Chief Inspector of Constabulary in Scotland and the Scottish Biometrics Commissioner are concerned about the apparent low level of CAID searches being undertaken. This finding has been highlighted by an earlier HMICS Strategic review of Police Scotland's response to online child sexual abuse in 2020 and complements the findings in this report related to both improved understanding among officers/staff of how biometric data support the criminal justice system and the effectiveness of RIST to produce actionable intelligence leads.

[39] See for example: https://www.scotland.police.uk/spa-media/j4rpeyug/biometric-custody-data-apr-jun-2024.docx, available at https://www.scotland.police.uk/access-to-information/biometrics/

Retrospective facial search volume data 2023-24

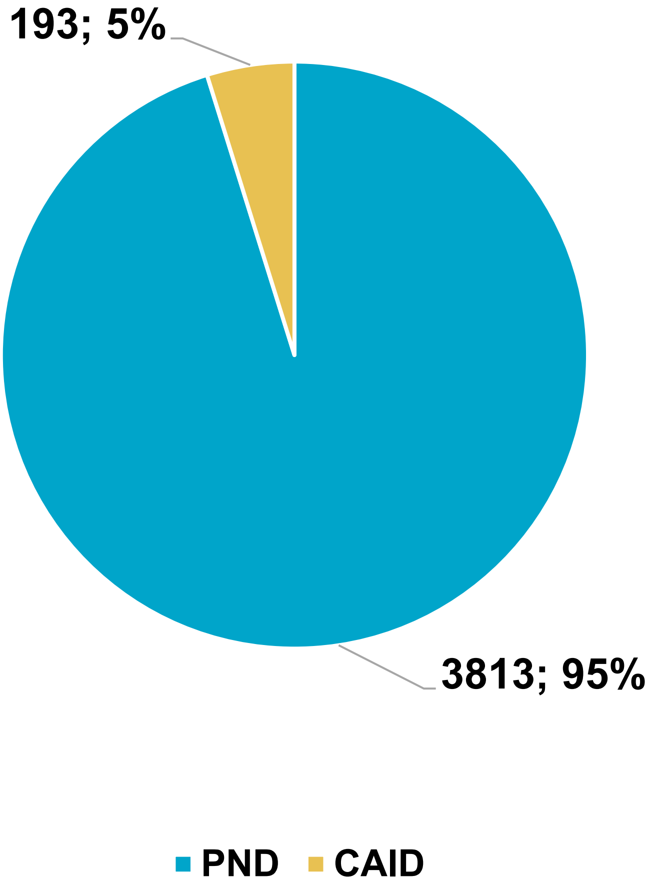
PND
There were 3813 retrospective facial searches for this period (April to March)

We found evidence of 57 positive matches, which is 1.49% of the total searches for the year.

CAID
There were 193 retrospective facial searches during the period (April to March).

This number includes 24 media verifications set, which is 12.4% of the total searches. Media verification is the process of human review and confirmation of a matched face from images or video footage.

Chart. Total volumes of retrospective facial searches by Police Scotland for 2023-24



PND comparative data

To provide comparative law enforcement data on the use of RIST by Police Scotland, the following are the figures for facial searches conducted by three forces from England and Wales during 2023–24: Greater Manchester Police, the Metropolitan Police, and South Wales Police.

Chart. Number of PND facial searches by police force.[40]

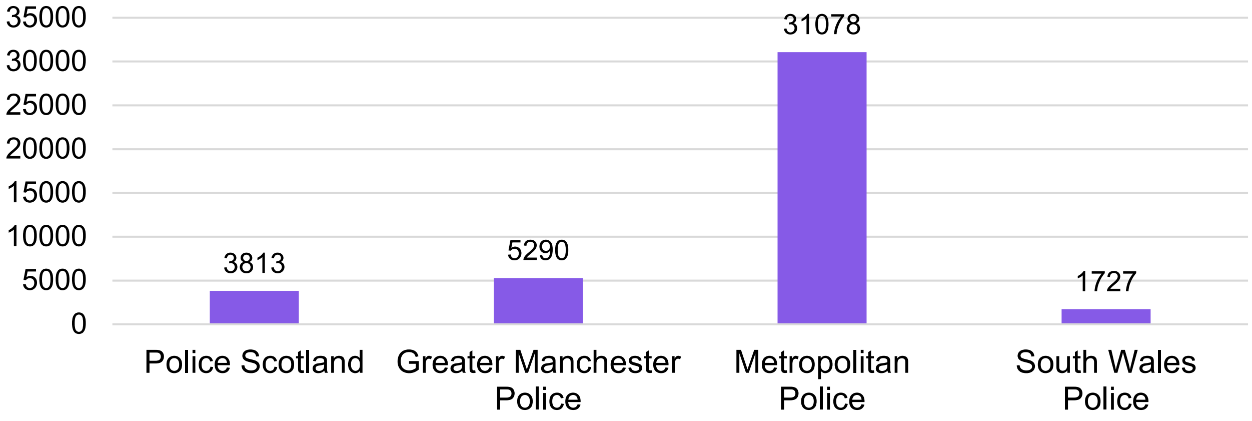


Table. Number of PND searches compared by national population, crime rate, officers by force, and PND users.[41]

	Police Scotland	Greater Manchester Police	Metropolitan Police	South Wales Police
Population of force area	5,463,000	2,911,000	8,855,000	1,333,000
Total number of crimes 23/24 per force	299,780	342,652	930,398	114,109
Total PND facial searches 23/24 per force	3,813	5,290	31,078	1,727
Crime rate per 1000 people	55.0	117.7	105.1	85.6
No. of crimes per PND facial searches	78.62	64.7	29.9	66.07
PND facial searches per 1000 head of population	0.697	1.81	3.5	1.29
Total officers per force	16,615	8,014	34,899	3,461
Total PND licences per force	340	566	2,263	238
PND auditors per force	1	1	Not known	2
Trained PND operators per force	320	582	2,645	238

[40] UK Home Office, statistics received directly from the Home Office to SBC in December 2024.

[41] This table was developed from data of Office for National Statistics in relation to Crime in England and Wales, Recorded Crime in Scotland by the Scottish Government and the UK Home Office data received in December 2024.

The comparative data suggests that Police Scotland are making proportionate use of the PND facial search functionality having conducted significantly less searches than smaller police forces such as Greater Manchester Police.

Case studies

The sanitised examples below provide a variation of how RIST has been utilised by Police Scotland to support the investigation of crimes and safeguarding of previously known child victims as well as reducing the requirement on human operators viewing entire catalogues of images of abused children.

In examples below, the value of searching custody images from across the UK is highlighted – in case study 1, the accused was not previously known, and the victim was unable to name the individual to police. In case study 1 and 3, the accused ordinarily resided in England therefore, it is highly likely that these individuals would be unknown to local Police Officers if circulated on internal identification bulletins.

The severity of the crimes which yielded a positive intelligence lead from PND facial searches range from solemn crimes such as Robbery, Abduction, Serious Assault, Sexual Assault to lower-level criminality such as Theft by Shoplifting.

Police National Database:

Case Study 1: VIOLENT CRIME

A door steward working in a licensed premises in the West of Scotland was assaulted by a patron on exiting the premises, struck over the head with a bottle causing a laceration to his face. The suspect was unknown to the victim. CCTV within the premises captured an image of the suspect which was subsequently used for a facial search against PND. The search provided a positive match of the suspect. The suspect was ordinarily resident in the Northwest of England but had previously had a custody image taken from Northumbria Constabulary. Permission was sought from Northumbria Constabulary, for Police Scotland to use this custody image in an ‘Emulator’ (Book of 12 images for identification) which was shown to the victim who made a positive selection, despite not knowing, or having previously met, the person responsible.

Case Study 2. SEXUAL ASSAULT

A tourist from East Asia visiting Glasgow was approached by an unknown local male and engaged in conversation before being sexually assaulted. The suspect requested the telephone number of the victim, and after leaving her, started sending sexually offensive messages/images to her, which was reported to Police Scotland. By use of the profile picture from the messaging app, the image was searched against PND, resulting in a positive match from a recorded custody image obtained 27 years ago. The male has subsequently been reported to the Crown Office and Procurator Fiscal Service for various sexual offences.

Case Study 3: ABDUCTION

Members of an organised crime group attended a property in the North of Scotland and abducted two individuals on suspicion of money being stolen from them, proceeding to torture the abductees by various acts of assault. Through enquiries conducted, an image was obtained of one of the males responsible, and this image was searched within PND. A male was positively identified, due to a previous custody image obtained by Police Scotland for offending in the South of Scotland, despite typically residing in the midlands area of England. The male was subsequently arrested and charged.

Child Abuse Image Database:

Case Study 4. INTERNATIONAL COOPERATION SAFEGUARDING CHILDREN

In March 2023, prior to Police Scotland utilising facial matching tool in CAID, Swedish law enforcement authorities requested assistance of NCA Victim ID team following a wider Europol operation uncovered a female suspected of being aged 13-16 years engaging in Category B sexual activity online. The female's ID was unknown, but CAID facial matching identified the same individual from a previous upload by Metropolitan Police to CAID (yet to be identified). The previous images depicted the female in a school uniform which was subsequently identified by NCA Victim ID team, as being within the West of Scotland. A package containing the school and potential name was subsequently disseminated to Police Scotland leading to a successful identification and safeguarding of the victim.

Case study 5. WELFARE TOOL

Facial matching as an officer welfare tool has proven to be invaluable in cases with multiple victims across multiple platforms/devices where officers are required to view multiple hours of child abuse imagery. One such case related to one offender who had been identified as abusing multiple children and after seizure of his device Victim ID were tasked to view every single child abuse image and video to determine how many children had been abused and what crimes had been committed. This included still images and video footage. Welfare in these cases is an enormous consideration as the scenes being viewed can be horrific and affect officers mentally over time. Facial matching was invaluable in separating out the footage of each child and vastly reduced the quantity of still images requiring to be viewed as well as the hours of video footage to be viewed. It also provided reassurances that all victims had been identified, safeguarded and that the Procurator Fiscal was able to charge with all crimes relating to each child. Time savings that the tool provided in this case cannot be measured but were vital to efficiently reporting to the required judicial timescales.

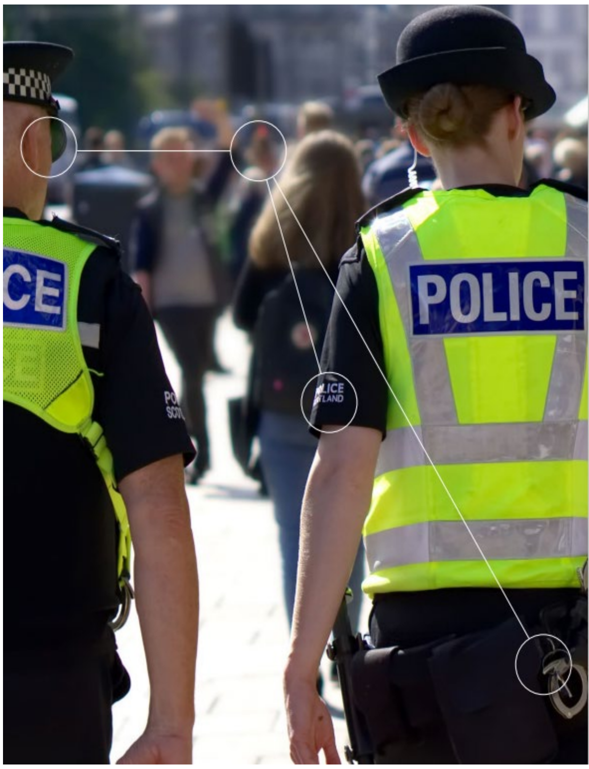
Chapter 5. Future legal and ethical challenges

Introduction

In an increasingly digital world, Police Scotland (and other law enforcement bodies) face several challenges, including balancing interoperability, autonomy, and the protection of the public order and human rights. This chapter explores the delicate interplay between these, examining the trade-offs, and opportunities as well as the importance that ethics and human rights remain at the forefront of digital governance.

Different or unified approaches

UK law enforcement, to keep up to date with new technological opportunities and advancements, currently adopt a disparate approach to new biometric technologies. For example, Police Scotland have never utilised Live Facial Recognition (LFR) whereas other UK Forces, notably South Wales Police and Metropolitan Police have been utilising LFR technology for several years.[42]



The reason for such disparate approaches is generally the lack of the development of a coherent biometrics strategy by police forces which sets out what they hope to achieve in the next 3-, 5- or 10-year period, including how they will work in partnership with their respective partners and forensic services provider.

In terms of retrospective facial search, the PND Facial Search tool has been a staple of all UK police forces, since 2014. At time of writing, Home Office Biometrics Programme (HOB), who provide biometric services to the UK government, are currently working on implementation of Strategic Facial Matching (SFM) Project, which will provide a new system and data migration of existing custody images onto a new national facial matching service for law enforcement purposes. This work also forms part of a wider ten-year programme which aims to deliver a central solution for law enforcement bodies to access and match data for both fingerprints, and facial images. It is also anticipated, that SFM, in addition to operating an improved algorithm for PND facial search searches, will add an additional functionality to support Officer Initiated Facial Recognition (OIFR) and Live Facial Recognition (LFR).

[42] For more information on LFR in England and Wales, see: https://researchbriefings.files.parliament.uk/documents/CDP-2024-0144/CDP-2024-0144.pdf

Police Scotland has been consulted by the UK Home Office on potential future use, and adoption, of SFM. This has been subject of a data ethics triage assessment and is being actively considered by Police Scotland. Subject to mitigating initial risks identified, this could be taken formally through their Rights Based Pathway, if adoption of the new system is progressed. In theory, this could provide Police Scotland with an improved, more accurate algorithm for retrospective facial search, resulting in higher match rates than is currently produced by PND. However, this report has identified a number of issues (e.g. state of custody images in CHS) which Police Scotland should consider prior to the adoption of new biometric-related technologies.

The introduction of new biometric technologies should follow a three-step process: first establishing strategic policy objectives, second, the formation of a robust framework for decision making and accountability and third, the commissioning of the specific technology, which is guided by such policy and framework.[43] In Scotland, the SBC Code of Practice provides a framework of standards for professional decision-making for responsible use of biometric related technologies. By adopting a balanced approach that integrates robust legal frameworks with technological innovation, law enforcement can harness new technologies such as image search technology while safeguarding our fundamental rights and democratic values.

Balancing interoperability

As Police Scotland transitions to new technologies, such as SFM, it is vital to balance the interoperability of national systems. There is no doubt that the integration of biometric databases, offer significant advantages in terms of cross-jurisdictional collaboration and information sharing. Regional decision-making is critical for tailoring responses to specific community needs and ensuring that enforcement actions reflect the devolution framework as well as UK policing priorities. For example, if Police Scotland decides to join SFM, it should be able to set their own rules around under what circumstances its own staff could access non-police images or any non-policing body (e.g. Border Force) could access Police Scotland images to ensure lawfulness, proportionality and necessity.

Ethics and human rights

The increasing integration of technology in law enforcement raises concerns about overreach and the erosion of fundamental rights, including the right to privacy.[44] While technology can be a powerful tool for enhancing security, unchecked surveillance risks undermining public trust in policing and creating systemic biases. To avoid this, law enforcement must ensure implementation of the SBC Code of Practice and guaranteeing that any technological solutions are proportionate, necessary, and subject to ethical review.

[43] For a further discussion of this process see: (Plastow, B) Increasing public trust in biometrics, 2024.

[44] For a discussion on retrospective facial recognition, see: Daragh Murray, 'Police use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Framework Law' (2024) Modern Law Review.

Expanding law enforcement's access to non-police images, such as those from passport or driving license databases, presents opportunities to enhance identification accuracy and investigative speed. However, this must be approached with due consideration to both the law and ethics. Without strong safeguards, including independent oversight, such measures risk edging society toward a surveillance State, undermining fundamental rights, where innocent citizens are exposed to the crawling reach of surveillance by the State.

An area which deserves more attention is the initial development of the technology, particularly considering the role of private business. We know that the vast majority of new technologies, including AI and facial recognition technology (FRT), are developed by the private sector. However, regulation and independent oversight in this sector is often considered limited or inadequate. In this context, the Parliament and government need to step up to enact appropriate legislation and guidance. Private business and the scientific research community can also play a key role in developing technical solutions that prioritise ethical considerations and promote respect for fundamental rights, including the protection of personal data.

Final remarks

In an increasing digital world, the future of law enforcement lies in achieving the right balance between the introduction of new technologies for public safety, balancing the interoperability of the digital systems, and safeguarding fundamental rights. For biometrics, public confidence should be maintained with transparency, robust governance and independent oversight. While the integration of biometric systems offers significant advantages, excessive centralisation risks sidelining local forces needs and domestic legal and policy frameworks. This, along with the issues highlighted in this report, should prompt significant reflection for policing in Scotland.

Scottish Biometrics Commissioner
Coimiseanair Biometrics na h-Alba

HMICS

Improving
Policing
Across
Scotland

Safeguarding our biometric future