I refer to the recent general call for evidence on the above topic and the specific areas of interest specified by the Sub-Committee. I also note the consultation background information on the Scottish Parliament website including that the Sub-Committee are aware that:

- Police Scotland has confirmed that it does not use and has not undertaken any trials of facial recognition technology in a live setting and that such technology has not been trialled, tested, or piloted in Scotland, by Police Scotland.
- Police Scotland has confirmed that it does however make use of the ‘Facial Search’ functionality within the UK Police National Database (PND) as a retrospective investigative tool.
- That the Police Scotland 10-year strategy Policing 2026, includes references to facial recognition technology.

Against this introductory context, I am happy to assist the Sub-Committee scrutiny by providing the following response from HMICS. For ease of reference, my comments and observations are structured to align directly with the areas of interest specified in the general call for evidence.

Additionally, as facial images of citizens held, captured or analysed on police databases clearly constitute ‘biometric data’, I would encourage the Sub-Committee to consider the contents of this particular submission by HMICS in parallel with my earlier submission of 23 July 2019 to the Justice Committee in relation to the Scottish Biometrics Commissioner Bill.

**Types of facial recognition technology used in policing**

Automated Facial Recognition (AFR) or Live Facial Recognition (LFR) is an advanced way of recognising people by using computers to scan their face with a camera as they walk by. Their use in policing in the UK has proved highly controversial, and some UK police forces have conducted trials of AFR/LFR since 2015 most notably the Metropolitan Police, Leicestershire Police and South Wales Police. HMICS is not aware of Police Scotland having conducted trials of or deploying such technology in Scotland.

The reason that such technologies are so controversial is that they facilitate the instant capture of biometric data from members of the public sometimes without their knowledge or consent. This type of technology is capable of conducting mass screening surveillance of thousands of citizens and therefore potentially has profound consequences for privacy, data protection and human rights. It also raises a range of ethical concerns. The Sub-Committee will also be aware that several UK police forces, outside of Scotland, have been publicly criticised by academics, regulators and the media for the use of automated biometric technologies which contain algorithms delivering unintended racial and gender bias in the results delivered by automated search transactions. This has led to some
facial recognition systems used by the police in England and Wales being described in the popular media as ‘dangerously irresponsible’.  

Quite separately, Police Scotland (and all UK police forces) use the ‘Facial Search’ capability within the UK Police National Database (PND) which is a system provided and approved for police use by the Home Office. This type of technology is not the same as AFR/LFR as it cannot be deployed in a live environment and it does not facilitate mass screening of citizens. Instead, it enables all UK police forces to upload an individual image of a suspect, and to use the automated software within PND to compare that single image against other images held on file from previous police custody episodes in an attempt to establish the potential identity of an offender. This technology has also proved controversial but for very different reasons, most significantly because many forces in England and Wales have failed to weed records of persons not subsequently proceeded against or convicted. The consequence is that the UK PND contains thousands of images of innocent persons. This has attracted extensive criticism including from the UK Commissioner for the Retention and Use of Biometric Data. 

In January 2016, HMICS published an audit and assurance review of the use of the Facial Search functionality within PND by Police Scotland. Our inspection found that Police Scotland had made very limited but appropriate use of this technology at that time. I would encourage the Subcommittee to study the detail of our 2016 report and the various findings which gave rise to our specific recommendations for improvement including a Scottish Biometrics Commissioner and a related Code of Practice for the acquisition, retention, use and disposal of biometric data.

The circumstances in which equipment is used to capture images

As AFR/LFR is not used by Police Scotland I shall confine my comments under this heading to how Police Scotland uses the Facial Search functionality within PND.

Firstly, it should be noted that the UK Police National Database was introduced by the Home Office in 2008. Its roots lie in the 2004 Bichard Enquiry into the 2002 murders of two children Holly Wells and Jessica Chapman by school caretaker Ian Huntley, and the resultant identified need for all UK police forces to utilise a common single intelligence sharing platform. Importantly, PND is not an evidential system.

In March 2014, the Home Office introduced a UK wide facial searching functionality within PND. Full details of how this system works is included in our 2016 report. However, in brief the system works by comparing an uploaded ‘probe image’ from a crime scene or incident, against a ‘gallery image’ previously placed on PND from UK police records. When searched, the system returns several possible matches which then require human assessment, comparison and investigation. The source of the ‘probe image’ is commonly from CCTV, cameras, mobile telephones or police body-worn video, but any digital image from any lawful source can be uploaded providing that it is of sufficient resolution to facilitate meaningful comparison.

---

The purpose of using the various technologies

As previously discussed, the purpose of AFR/LFR is to facilitate mass surveillance for a specific policing purpose. In a policing context, forces in England and Wales have deployed such technology at public events and have sought to compare facial images of the general public against images held on police records. By contrast, the purpose of PND Facial Search is to speed up and semi-automate the otherwise manual identification of specific potential suspects. Regardless of the outcome of a search, the individual probe images are not retained on PND after the search has been conducted.

Data protection, security, retention and equalities and human rights considerations and the legal and regulatory basis

In relation to AFR/LFR and its use in England and Wales there have been numerous concerns raised about the use of such systems. This recently led to the first legal challenge in the UK on one specific application of facial recognition (AFR Locate) by South Wales Police. On 04 September 2019, the High Court in Cardiff ruled that the particular use in question was lawful and did not breach Article 8 rights as the actions were subject to specific legal controls contained in primary legislation (including the data protection legislation), statutory codes of practice and the published policies of South Wales Police and were legally justified. In reaching its conclusion and justification, the court noted that on each occasion, it was deployed for a limited time, and for specific and limited purposes. The court also noted that, unless an image of a member of the public matched a person on a watchlist, all data and personal data relating to it was deleted immediately after it had been processed.1

In the absence of any specific legal framework or Codes of Practice in Scotland, it is highly likely that any future deployment of AFR/LFR in Scotland would be contested and that the lawfulness of a specific application would need to be determined in the Scottish Courts. In this regard, it would be essential not only that the actual activity by the police itself was lawful, but also that the specific technology solution in question was reliable and non-discriminatory. Another issue for Scotland, is that unlike the rest of the UK there is still no primary legislation giving authority to the police to photograph persons brought into police custody, and hence the legality of the comparison images could be challenged. This identified gap in the law led to a recommendation (recommendation No 1) from our 2016 PND report that Scottish Government should work with Police Scotland and the Scottish Police Authority to consider legislative provision in relation to the retention and use of photographic images by the police. As highlighted in my related earlier response to the Justice Committee on the Scottish Biometrics Commissioner Bill, this situation persists and is an ongoing risk requiring careful management.

Oversight, governance and transparency

In our 2016 report, HMICS noted that legislation was not keeping pace with rapid advances in biometric technologies and we identified a need for improved legislation and better independent oversight and transparency around the police use of biometrics in Scotland. Our 2016 report contained four recommendations, including the establishment of a Scottish Biometrics Commissioner to address the issues of ethical and independent oversight over biometric databases and records held in Scotland, with flexibility to embrace future technologies and relevant codes of practice. This would include biometric technologies such as AFR/LFR if subsequently adopted for use in Scotland.

---

As highlighted in our 2016 report, and the subsequent report of the Independent Advisory Group on the use of Biometric Data, a Scottish Biometrics Commissioner could also build capacity and resilience within Scotland to explore emerging human rights and ethical considerations around the application of automated biometric technologies by other public agencies most notably public space CCTV surveillance systems. Clearly new and emerging technologies escalate the value and possibilities around the use of biometric data and when combined with the development of underpinning codes of practice, my view is that the creation of an independent Scottish Biometrics Commissioner could both safeguard and futureproof what will undoubtedly continue to be a fast and evolving scientific landscape.

I trust that this submission is of value to the Justice Sub-Committee in considering the specific issue of facial recognition technologies, and I confirm that I would be more than happy to participate in subsequent verbal evidence sessions on this matter.

Mrs. Gill Imery QPM  
Chief Inspector of Constabulary