Law Society of Scotland

70 Years 1949-2019

Call for Evidence on Facial Recognition:

How Policing in Scotland makes use of this technology

1 November 2019

Introduction

The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders and our membership.

Our Criminal Law Committee welcomes the opportunity to consider and respond to the Justice Sub-Committee's Call for Evidence on Facial Recognition: How policing in Scotland makes use of this technology. The focus of the Call for Evidence centres on how policing in Scotland makes and should make use of facial recognition technology and whether that use is lawful, ethical, proportionate and transparent. The committee has the following comments to put forward for consideration.

General

Police Scotland's 10-year strategy, Policing 2026[1] refers to the role of facial recognition as part of their future service delivery to address the growing and different demands of 21st century Scotland.

There is a need for investment in Police Scotland's forensic capacity to support the changes in criminality. Facial recognition is one example of the development in forensic science. Police Scotland want "to get the best from science and technology [that] support[s] the effectiveness of policing and the delivery of justice in Scotland." These advances in technology also require their staff to be equipped with the necessary skills to undertake these roles.

At the outset, there is an obvious overlap between this Call for Evidence and the scope of the Scottish Biometrics Commissioners Bill (the Bill). In that Bill's Call for Evidence, we recognised that the developments in biometric data were fast moving and that there would be considerable benefit in producing a regulatory framework to include facial recognition. Such a regulatory framework would require to ensure:

- Where there were experimental trials or development of appropriate new technologies that they are conducted in such a way as to support the operational choices being made by the police about the methods to use and the biometric data that is to be obtained and

[1] https://www.scotland.police.uk/assets/pdf/138327/386688/policing-2026-strategy.pdf

- support for the police development of artificial intelligence or machine-based learning through the application of data analytics to biometric data, including the technology used for facial recognition or intelligence gathered.

This was also pertinent to the recent consultation on the Strategic Police Priorities for Scotland where we recognised that there was a need to future proof the legislation such as the Bill to take account of the advances in technology and the use of artificial intelligence.[2]

Though there are obvious public benefits to be gained from such advances in technology, we are concerned that certain steps are taken to ensure that:

- There is careful evaluation of the proposed use of any new technology before it is deployed
- Robust evaluation is carried out to the appropriate scientific standard for using such technology before decisions regarding its use are put in place
- The public are served by principles of openness, inclusivity and engagement to maintain public trust
- Respect for equality, dignity and human rights
- Addressing concerns and outcomes which would require trials to continue to be subject to ethical appraisals and respond to developing concerns[3]

We note that Police Scotland has not yet undertaken any trials of facial recognition technology in "a live setting through, for example, public space cameras, CCTV or other means, has not been trialled, tested or piloted in Police Scotland."[4] These steps are essential in going forward to ensure that the use of such technology is appropriate. It would appear appropriate to take cognisance of other experiences that have arisen from the use or intended use of such technologies which we discuss below.

The sorts of issues that may arise can be seen quite readily from the recent problems over the Metropolitan Police Service having supplied images for a database used to carry out facial recognition of people who visited Kings Cross.[5]

Obtaining public confidence is essential. That means the balance has to be maintained between the inevitable invasion of individual privacy that arises with the use of facial recognition, the potential clash with Article 8 of the European Convention on Human Rights and the public and State benefit that derives from the use of such technologies in furtherance of the detection of crime.

The type of facial recognition technology used by the police service, the circumstances, and any implications. For example, Police Scotland accessing facial

[2] Strategic police priorities for Scotland https://www.lawscot.org.uk/media/363788/19-10-03-crim-strategic-police-priorities-for-scotland.pdf

3. These largely echo the Report from the London Policing Ethics Panel[3] which recommended a similar approach. that steps needed to be taken: http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

[4] Call for Evidence on Facial Recognition

[5] https://www.bbc.co.uk/news/technology-49586582

recognition images from CCTV cameras, national databases, body worn video cameras, and potentially mobile phones.

Taking the technology point first, this is important from the perspective of ethical and transparent processing in that many forms of facial recognition technology currently in use are reported as displaying different behaviours for some groups (such as for females or members of minority ethnic groups) than they do for the “control” group which is typically white and male. Transparency around the technology being proposed is important to allow any such in-built biases to be tested and challenged. This is a concern that is also recorded by the London Policing Ethic Panel’s report where it recorded;

“Almost half of respondents thought the technology would lead to personal information being collected more often about some groups than others. Younger people were less accepting of police use of [facial recognition] than older people, and people from Asian and Black ethnic groups were less accepting than those from White groups.”[6]

Technology has an impact on the intrusiveness of the activity, particularly if something goes wrong and a person is mis-identified. The consequences for an individual who is mis-identified by a retrospective analysis of CCTV footage are likely to be much less significant than for a person mis-identified by a system connected to a police officer’s body-worn camera and carrying out matching activity in real time.

Technology has an impact in terms of the extent to which it can minimise or maximise the collateral intrusion of such as system, i.e. the capture and processing of data relating to people of no interest to whatever is being investigated. It is recognised that true transparency in this area is problematic. Critics may want to be able to analyse the matching algorithms used by the systems. These are likely to be considered as commercial sensitive intellectual property by the systems’ developers. In the main, facial recognition software is likely to be a “black box” technology which cannot be analysed other than in terms of its outputs. This is important in assessing the lawfulness and proportionality of the use of this technology.

Police Scotland do not presently hold the majority of the images which would be of particular use when deploying facial recognition technology. Public space CCTV, for instance, is generally operated by local authorities under section 163 of the Criminal Justice and Public Order Act 1994 (or by companies/trusts set up by local authorities to manage CCTV systems on their behalf). This is an important safeguard against any disproportionate intrusion through over-use of facial recognition software, as the local controllers of CCTV systems would need to be satisfied that the police had a genuine reason for accessing footage and were not simply operating facial recognition software as a matter of routine.

The use of mobile phone footage is also interesting. It is not clear what is meant. Does it refer to mobile phones being used by police officers themselves or the police being able to access the phone footage of private citizens (which would be particularly intrusive and something only to be done under a warrant)?

[6] http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf

The use of phones by the police raises broadly the same issues as does the use of body-worn cameras, though the recording on a mobile phone by a plain-clothes officer could stray into directed surveillance and accordingly need to be authorised under the Regulation of Investigatory Powers (Scotland) Act 2000.

We have concerns round the use of facial recognition technology on images which have been published on the Internet (particularly, but not exclusively, on social media). There are scenarios where this would be of great use to an investigation but given the proliferation of images on the Internet and the ease and invisibility with which these can be accessed by anyone, there need to be specific safeguards against wholesale or routine analysis of online images by the police.

The circumstances in which equipment is used to capture images, for example the use of body worn video cameras at major events, such as protests and football matches.

This question seems to presuppose that the equipment will be used in connection with public space CCTV footage. The deployment of public space CCTV may be sufficiently mature to require no further safeguards, but it would be more sensible to consider under which circumstances it would be appropriate to use facial recognition software on other types of data, such as the online data.

The purpose of using facial recognition technology. For example, Police Scotland's practice of sharing images with UK police forces through the use of the Police National Database (PND), which has a 'facial search' facility.

Given our observations regarding Article 8 of ECHR, the only legitimate purposes for these activities would have to be justified in terms of Article 8(2), i.e. for the purpose of preventing or detecting crime or of preventing disorder; in the interests of public safety; or for the purpose of protecting public health.

Any data protection, security and retention implications, and the equalities and human rights implications of the use of facial recognition technology (either by Police Scotland or by private sector entities on their behalf).

There are a number of data protection implications that arise from the use of facial recognition technology that covers the whole cycle. That includes privacy by design in choosing a system, data protection impact assessment (and the need for ICO approval)[7] ahead of its operational use which would also need to be assessed publicly, provision of the appropriate privacy statements to those who may be affected by the

[7] The data protection impact assessment should be able to identify equalities and human rights issues arising from the system.

technology, secure data capture and the storage and proper consideration of how long data needs to be stored for (assuming it needs to be stored at all, in the case of real time analysis).

A number of these items may well fall within the scope of the Scottish Biometric Commissioner Bill.

The legal and regulatory basis that Police Scotland rely upon to use facial recognition technology

The legal and regulatory basis for the use of facial recognition in Scotland on which Police Scotland will rely needs to be developed in the light of experience from other jurisdictions. A UK court has considered the issue of facial recognition[8] for the first time in the world. There are implications arising from that judgment for Scotland although it was specific to an extent in considering the policing policies in South Wales Police and that existing legal framework relating to facial recognition. There was a benefit n considering facial recognition in its trial phase and before it is rolled out. The challenges that were considered were in common with those that would be anticipated to arise in the Scottish courts which include data protection, human rights and the Equality Act 2010. Ultimately, the court found that any infringement of Article 8 ECHR was in accordance with the law. Any data collected for facial recognition though it comprised personal data was compatible with Article 8 ECHR since its use satisfied the conditions of lawfulness and fairness. There was insufficient evidence to justify any public sector equality claim.

We would stress that though the decision in that case may have found in favour of the police, that seems far from the end of the discussions. There are calls for a facial recognition technology code of conduct to be produced for England and Wales while Liberty[9] who brought the case are campaigning for a ban. Elizabeth Denholm the Information Commissioner has indicated her concerns about the use of a technology that relies on huge amounts of sensitive personal information."[10] The principles of the case are of relevance but much will depend on the framework and use that Police Scotland seek to put in place.

Further afield, it should be noted that a moratorium currently exists in California where The Body Camera Accountability Act blocks police from using face recognition technology on officer-worn body cameras. This is a state-wide, three-year ban on police body camera use of face recognition surveillance. Concerns there had included:

[8] R (on the application of Bridges) v Chief Constable of South Wales [2019] EWHC 2341 (Admin)

[9] https://www.libertyhumanrights.org.uk/

[10] https://www.bbc.co.uk/news/uk-wales-50251643

"Face-scanning police body cameras have no place on our streets, where they can be used for dragnet and discriminatory surveillance of people going about their private lives, including their locations and personal associations."[11]

Concerns have also been raised in the House of Commons Science and Technology Committee where they flagged up that there needed to be a "clearer legal framework [for England and Wales] outlining how Automatic Facial Recognition (AFR) can be deployed [that] would support law enforcement practitioners." The Bill provides Scotland with that opportunity.

The oversight, governance and transparency of Police Scotland's use of facial recognition technology

These would tend to be matters for the Bill but need to be resolved before the use of facial recognition becomes operational.

[11] https://www.aclu.org/press-releases/california-blocks-face-recognition-police-body-cameras

For further information please contact:

Gillian Mawdsley

Policy Executive

Law Society of Scotland

DD 0131 4768206

gillianmawdsley@ntlworld.com