JUSTICE SUB-COMMITTEE ON POLICING

FACIAL RECOGNITION: HOW POLICING IN SCOTLAND MAKES USE OF THIS TECHNOLOGY

WRITTEN SUBMISSION FROM DR GARFIELD BENJAMIN, SOLENT UNIVERSITY

Background

Facial recognition is a contentious issue currently undergoing massive public and regulatory scrutiny. Police Scotland's approach so far has been highly commendable, for four reasons:

- Putting their proposal forward for legal and public scrutiny;
- Awaiting regulatory frameworks such as the Scottish Biometrics Commissioner Bill;
- Not undertaking public trials until after these processes; and
- Acknowledging related existing uses such as retrospective facial searches.

It is therefore hoped that the Sub-Committee and Police Scotland will be sensitive to the many issues surrounding facial recognition, and choose to support rights, freedoms and diversity rather than entrench automated surveillance and control of public spaces.

Global context

Precedents are currently being set across the world that establish the need for limits and careful consideration about the use of facial recognition technologies. Although the recent case of South Wales Police's use of facial recognition trials in public was deemed lawful, the judgement did acknowledge that collection of images classes as personal data and should follow all relevant regulations.[1] There is also an Automated Facial Recognition Technology (Moratorium and Review) Bill currently passing through UK Parliament (second reading in the House of Lords).[2] Beyond legal and regulatory environments, the Ada Lovelace Institute recently released a report showing public opposition to facial recognition - over half wanted some form of restrictions and almost one third wanted police use to halt altogether.[3]

Elsewhere, a moratorium on facial recognition technology has been passed by Morocco[4] and for police use for three years by California,[5] while a broader moratorium bill is currently going through in Massachusetts.[6]

[1] https://www.judiciary.uk/judgments/r-v-the-chief-constable-of-south-wales-police-and-others/
[2] https://services.parliament.uk/bills/2019-20/automatedfacialrecognitiontechnologymoratoriumandreview.html
[3] https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/
[4] https://www.cndp.ma/images/deliberations/deliberation-n-D-194-2019-30-08-2019.pdf
[5] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215
[6] https://malegislature.gov/Bills/191/s1385

Known technical and ethical issues

Researchers have found strong racial and gender bias in a range of facial recognition systems,[7] [8] including an 80% error rate with the system used by London Metropolitan Police.[9] [10] This included not only technical problems but issues with deployment, transparency and oversight.

Ethical concerns are perhaps more nebulous but also very clear. The UK Biometrics Commissioner has stated that facial recognition and other biometric systems are "an intrusion into an individual's privacy".[11] At a time when privacy legislation - such as the GDPR - is making some progress in protecting citizens' rights to privacy, widespread deployment of facial recognition would be highly problematic to implement and a step backwards for freedom.

Facial recognition is at once intimate and public. It takes advantage of being in public spaces by using identifying markers that are strongly tied to one's family and racial background. The face plays a key role in society for building authenticity, identity and trust, all of which is placed at risk by these technologies. Even for trials, it cannot be considered consent (no matter how well informed) if that consent is required for access to public spaces.

There is an inversion of innocence with facial recognition. When a member of the public enters a space monitored by facial recognition, they are automatically placed in a police lineup. This fundamentally changes the role and power of the police, from one in which evidence is a case must be built to prove guilt into one in which everyone is assumed guilty all the time. Should Police Scotland (or, indeed, any police force) go ahead with the use of facial recognition then they are making an active choice to shift policing into a state of constant surveillance, forcing citizens to live beneath a constant machinic gaze. We must ask ourselves the cost, in terms of freedom, trust and inclusivity, of any surveillance technology. And we must not only regulate but develop and test such technologies according to the ethical and societal values we wish to embody.

Relational issues

No technology exists in a vacuum. It is always embedded in a complex array of technical, regulatory and social relations that must be taken into account. A number of guiding principles and connections with other issues in turn raise some highly problematic questions concerning facial recognition, particularly when considering implementation in practice.

[7] http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
[8] https://ironholds.org/resources/papers/agr_paper.pdf
[9] https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns
[10] https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf
[11] https://www.gov.uk/government/news/automated-facial-recognition

Children's privacy

The UK Children's Commissioner released a report on children's privacy and the shocking amount of data that is collected and shared about children, often without their permission or even knowledge. The report highlights how more needs to be done to ensure that children's privacy is respected, and researchers have found that children want greater transparency over their data[12]. This is essential not only for protecting their rights but for helping children to develop as aware and engaged digital citizens.

But how would the implementation work to protect children? Having a children's database to check against is obviously counterproductive. But any attempt to automate detection of a child in order to exclude them from analysis still entails biometric invasion and raises further questions - what determines the characteristics for a 'child face'? What happens for children who look 'too grown up' and are therefore discriminated against by being treated as an adult?

Automated policing

Facial recognition is a process of automation, but it risks being used as a gateway to excessive automation that lessens both the role and responsibility of trained human officers. A machine learning system building an evidence case itself is a massive leap from using such systems to help officers build a case, and requires sensitive interaction with regulations and public expectations around due process and police integrity.

But page 41 of Police Scotland's 2026 Strategy suggests that as part of facial recognition use, "the AI begins to build an evidence case"[13]. There is much literature on the risks of AI decision-making, much of it focused on two key issues. One is that computer systems can make major mistakes that are not immediately obvious or occur too quickly or as part of too large a dataset for humans to notice. This has happened in stock markets with flash crashes instigated by glitches or miscommunications between automated systems. The other issue is the risk of discrimination. As machine learning data is generated from existing human data, it tends to escalate existing bias and societal inequalities. Allowing machines to build evidence cases greatly increases this risk.

Resource allocation

Facial recognition technologies, while a current source of hype amongst tech companies, are a significant investment. Budgetary concerns appear prominently in Police Scotland's 2026 Strategy. To avoid misappropriation of public funds, any system bought or commissioned would have to prove its success 'in the wild' in terms of error rates and effectiveness in actually helping police investigations. There are also ongoing concerns over updates and maintenance, with the continued use of out-of-date (potentially highly biased or flawed) systems raising major issues for human rights.

[12] https://blogs.lse.ac.uk/parenting4digitalfuture/2019/09/18/childrens-expectations-regarding-fair-treatment-of-their-personal-data/

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

But there is much evidence to suggest that the current state of the technology is far from ready for deployment. Systems still have extremely high error rates. Not only do false positives (for example, the ACLU found that 28 members of the US Congress were matched to criminals by a leading facial recognition algorithm[14]) introduce bias, discrimination and unfair harassment, but they also waste police time. There is no compelling case that facial recognition is a valid use of public funds or police resources.

Inter-organisation cooperation

Governmental and police agencies naturally cooperate across the UK. This combines appropriate jurisdictional constraints with the need to work together on increasingly connected issues. Such cooperation must therefore be subject to all relevant regulations, taking the most restrictive, sensitive and respectful approach rather than the most permissive.

But the differences between judicial areas of the UK make such relations problematic. There have recently been high profile cases of disagreements between, for example, Scottish and English courts.[15] The combination of facial recognition with other systems such as existing databases or body cameras further embeds these problems in broader contexts. The corporate basis of these systems only adds more difficulties in justifying the use of such privacy invasive technologies, particularly when it comes to accountability for errors and their societal impact.

Recommendations

I submit to the Sub-Committee the following recommendations:

> At a minimum, Police Scotland should continue to assure the public that no trials will be conducted before significant regulatory frameworks (with public consultation) have been put in place;
> A moratorium should be put in place by Scottish Parliament on the use of facial recognition in public spaces. This should ideally be permanent, or at least until significant regulatory frameworks have been put in place;
> Should facial recognition ever be deployed in Scotland, an independent review and commissioner should be established, including mechanisms for academic and public debate on evolving ethics incorporating diverse perspectives;
> Police Scotland should focus their already constrained resources on supporting officers more directly to perform their duties and build trust with communities.

Facial recognition systems are technologically flawed, legally dubious and ethically reprehensible. Their deployment stands only to entrench bias, harass innocent members of the public, and shift society into a police state with no respect for bodily or privacy rights.

Dr Garfield Benjamin

[14] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
[15] https://www.instituteforgovernment.org.uk/explainers/court-challenges-prorogation