The Type of Facial Recognition Technology used by the Police Service, the Circumstances, and any Implications

Engaging the Public

1. Facial data differs from other biometrics currently in use, such as fingerprints or DNA, in that it can be collected remotely and stored without the knowledge of the individual being scanned. This significantly impacts upon individual privacy if facial recognition (FR) systems are used in public spaces.

2. Public approval is therefore vital if FR systems are to be used in Scotland. It is unclear however what level of public awareness and understanding of FR currently exists in Scotland, and there is a paucity of research on public attitudes. A recent UK survey conducted by YouGov on behalf of the Ada Lovelace Institute does however provide some indications. This study concluded that public awareness of FR is high, but knowledge of it is low, which warrants a more informed debate. The survey found a notable fear of the normalization of surveillance, and found no unconditional support for police deployment of FR. Public support was instead conditional ‘upon limitations and subject to appropriate safeguards’.

3. I believe that FR should not be used in Scotland before public attitudes are suitably assessed, and not without informed public approval, and then only with appropriate safeguards in place. Citizen’s juries could play a role in the public engagement process, although the outcomes of such juries should only be considered as advisory and must be accompanied by methodologically rigorous research. The proposed Scottish Biometrics Commissioner could be very well placed to commission research on Scottish public attitudes to FR, and to lead on public engagement activity.

Testing Facial Recognition: Reliability, Validity and Ethics

4. Further to my evidence to the Justice Committee on 24th September 2019, I believe establishing the reliability and validity of any type of biometric system is fundamental to ensuring ethical use. This is particularly germane with regard to FR, so that individuals do not suffer the possible consequences of algorithmic bias and false positive identification, which remains a major concern. Both the Surveillance Camera Commissioner and the UK Biometrics Commissioner have expressed the

---

1 Ada Lovelace Institute (2019).
2 Ibid.
view that systems should be appropriately tested. Designing tests however requires careful consideration as technical and ethical issues arose in FR tests conducted in England and Wales.

5. The Metropolitan Police Service (MPS) expressly sought to test the technical aspects of FR, yet testing occurred via police operations. During the MPS trial, research objectives appear to have been conflated with police objectives, leading to members of the public being seriously inconvenienced, with evidence of possible discrimination. Mixing the testing of FR with operational deployment appears to have created some significant ethical issues concerning consent, legitimacy and trust. The apparent conflation of objectives obscures an important distinction between an individual’s right to withhold consent to participate in research, and their consent to the use of technology in police operations. From the point of view of research ethics, the avoidance of cameras may indicate an individual’s right to withhold consent to participate in a trial or to uphold their right to privacy. Such behaviour may however be seen quite differently from a policing point of view, possibly raising suspicion.

6. The testing of any new FR systems in Scotland should be subject to the most stringent consideration. The Scottish Biometrics Commissioner could lead on designing FR tests and should seek assistance from relevant experts, including an Ethics Advisory Group.

The Circumstances in which Equipment is used to Capture Images

Public Consent

7. Civil society organizations such as Liberty and Big Brother Watch have criticised the use of FR technology by the MPS, South Wales Police (SWP) and other forces at gatherings including sports events, music concerts and conventions. SWP have recently used FR to monitor over 20000 football fans at a Cardiff City versus Swansea City match (I note protests which have occurred at Scottish football fixtures against FR). SWP also deployed FR at a protest against an arms trade convention in Cardiff, which raised concerns over whether such use could dissuade the public from exercising their right to freedom of expression or legitimate protest.

8. Questions of informed consent relate to how well the public may be informed by police forces deploying FR technology, and the kind of time-frame in which publics may be able to exercise consent. The use of FR in public spaces also raises uncertainties over the agency of individuals to exercise different choices, such as taking different routes to avoid cameras, and how police might interpret such behaviour. Such issues should be included in public discussions.

---

5 Big Brother Watch (2018); Fussey & Murray (2019).
7 Big Brother Watch (2018); Liberty (2019).
8 Big Brother Watch (2018).
9 Big Brother Watch (2018); Fussey & Murray (2019).
Police Decision-Making

9. Police deployment in England and Wales has raised concerns about the consistency of decision-making processes involving FR. Fussey & Murray (2019) identified multiple and conflicting types of decision-making practices employed by the MPS.10 The use of multiple adjudicators in a control room to confer on possible matches, which sometimes led to differences of opinion; communicating a possible match to street level officers, which sometimes led to communications issues over whether this represented an instruction to intervene or merely to maintain observation; and equipping street-based officers with handheld devices which could alert them to a possible match. It was reported that in these latter instances, street-based teams took a decision to intervene even though control room-based teams had decided otherwise.

10. The experience of the MPS raises questions over who should be accountable for taking decisions to intervene based on FR data, what decision-making protocols should be devised, and what criteria should be used to make decisions. If instituted, the Scottish Biometrics Commissioner could play a key role in shaping decision-making via a Code of Practice.

Operational Learning Curves and Assessing Outcomes

11. Davies et al’s (2018) study highlighted significant learning curves concerning the operational use of FR by SWP. Davies et al found that ‘multiple organizational reforms and innovations were required’ before FR operated to a satisfactory level.11 Training was identified as an issue during the SWP deployment. The amount of formal training given to initial operators appears to have been brief, and many subsequent operators used FR without any formal training.12 A host of technical and practical issues only became apparent following operational deployment.

12. While some of these technical issues could have been addressed in non-operational testing phases, it appears that operators often had to responsively adapt their practice at the scene. The existence of such learning curves suggests that the Scottish Biometrics Commissioner, if brought into office by future legislation, should liaise with stakeholders to address operational issues regarding FR if it is approved for use. While pre-operational testing may identify some issues, liaison should focus on sharing experiences and providing a learning network. Any proposed Code of Practice should be reviewed in the light of possible operational contingencies which may arise in the course of using FR.

---


11 Police operators had to gain a certain amount of familiarity with FR technology over repeated operations, and there were several technical issues which impacted upon performance. The FR systems could not be used without first adjusting a series of technical settings to gain satisfactory performance. For example, image similarity scores had to be adjusted to avoid too many false positives. Adjustments also had to be made to settings such as ‘faces per frame’ rates, image resolution, and the quality and type of images included within watchlists (Davies et al 2018, p.17). Too many false positives appeared to cause frustration among operators.

12 Ibid., p.16.
13. Concerns remain about the way in which automated FR systems learn how to compare images. Algorithms remain black-boxed and it is often impossible to determine how they learn to process matches. The possibility that technology may enable these systems to 'explain' their judgements should be encouraged.

14. I follow Purshouse & Campbell (2019) in urging that, if approved, police publicise the use of FR in operations, and regularly publish data regarding the performance of technology, including numbers of false positive matches and numbers of interventions based on false positive matches.

The Purpose of using Facial Recognition Technology

15. The use of FR technology for policing purposes has been justified in various ways: for benefits of detection, deterrence, crime displacement and disruption. These reflect clear differences in purposes, ‘requiring distinct necessity calculations’, and indicate how decisions to deploy FR are highly contextualized. Hence consideration must be devoted to the nature and structure of decision-making, and the organizational context within Police Scotland regarding the deployment of this technology. The use of FR systems should strike a proportionate balance between individual privacy and dignity on one hand, and public safety on the other. Proportionality should however be thought of as a calculation and not a value, and may be dependent on a host of local circumstances and contexts, including the intended policing purpose, the location of the public space being monitored, and the public purposes for which space is being used (e.g. political demonstrations, sports events etc).

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)

16. FR systems may involve the construction of watchlists of suspected persons against whom facial data recorded in public spaces may be compared. Determining whether an individual should be placed on a watchlist constitutes a significant threshold moment. Fussey & Murray (2019) found that in England and Wales, persons were flagged by FR for serious offences that had already been dealt with through the criminal justice system. Some of these persons were still however wanted in relation to minor offences and were arrested accordingly. It was questionable however whether these lesser offences would have been sufficient to justify inclusion on the previous watchlist. Clear criteria for inclusion of individuals on watchlists should be formulated before FR technology is deployed. Davies et al’s (2018) study of SWP’s use of FR recommended that decisions around watchlist size and composition should be made public for the

---

13 Purshouse & Campbell (2019);  
16 Ibid.  
17 Ibid.
purposes of public accountability.¹⁸ The issue of including vulnerable persons on
watchlists also needs consideration.¹⁹

17. The possibility of using FR to infer family membership on the basis of facial
comparison may need to be addressed in the near future. Bowman & Grindrod
(2019) claim that ‘it is almost inevitable that the faces of criminals, terrorists, and any
persons of interest to the security services, that are caught on public or private
CCTV and by other surveillance means, will be matched to their kin on national
databases, such as the Police National Custody Image database.’²⁰ Such a
possibility presents a serious challenge to privacy rights and informed consent.
Using FR to infer family kinship could present the risk of inferring family links
between individuals who had been unaware of them (for example, an individual
discovering a sibling of whom they were previously unaware), which may have
serious consequences for a person’s sense of identity or family ties if adulterous
behaviour is suspected. The possibility of false-positive matches could compound
such a situation further.

The Legal and Regulatory Basis that Police Scotland rely upon to use Facial
Recognition Technology

18. The UK Government have claimed that current use of FR complies with a
number of pieces of legislation, including the 1998 Human Rights Act, the 2000
Freedom of Information Act, the 2012 Protection of Freedoms Act, the 2018 Data
Protection Act and the 2000 Regulation of Investigatory Powers Act.²¹ However, in
response to a written parliamentary question from Layla Moran MP, Nick Hurd, the
UK Minister of State for Policing, responding for the Home Office, stated ‘there is no
legislation regulating the use of CCTV cameras with FR.’²² The Surveillance Camera
Commissioner has also raised the issue of the lack of a clear statutory footing for
FR.²³

19. The High Court in Cardiff has recently ruled that the use of FR by SWP was
lawful and that it was consistent with human rights and data protection laws.²⁴ This
ruling may however be appealed, and it should not be assumed to have ended the
debate concerning the legality of FR.²⁵ The Scottish Government should therefore
continue to consider whether FR technology is lawful in the Scottish context.

20. The Scottish Biometrics Commissioner Bill, if passed, will bring into being a role
to oversee the police use of all biometric technologies. The Scottish Biometrics

¹⁹ Ibid., p.19.
²¹ Written evidence submitted by Baroness Williams of Trafford, Minister of State for Countering
Extremism, Home Office (WBC0009), to House of Commons Science and Technology Committee,
The Work of the Biometrics Commissioner and the Forensic Science Regulator, 19th Report of
Session 2017-19.
²³ Ibid.
²⁴ Bridges, R (on application of) v. Chief Constable of South Wales Police [2019] EWHC 2341
(Admin); Technology Law Dispatch (2019).
Commissioner will formulate a Code of Practice for which police bodies will have regard. The proposed legislation does not cover the use of biometrics by private-sector organizations, which could include, for example, private security firms. In addition to ensuring that legislation is truly enforceable and meaningful, legislation should ensure that FR use (if publicly approved), is only used by Scottish police bodies and not delegated to private organizations. Further consideration should also be given as to whether legislation concerning FR should extend to other parts of the Scottish Criminal Justice System, such as the Scottish Prison Service.

21. Based on the experience of England and Wales, it is likely that Police Scotland may have to rely on the private sector to supply elements of technology for FR, such as automated recognition software.\textsuperscript{26} This raises questions over who may be accountable for the reliability and validity of such systems under future biometrics legislation. Technology producers have made ambitious claims that FR can be used to anticipate behaviours, detect emotions or even infer sexuality.\textsuperscript{27} I urge that such claims be subject to the utmost critical scientific scrutiny. I am concerned that such claims could reflect commercial interests at the expense of ethical and scientific rigour. The Code of Practice and attendant legislation should compel private sector suppliers to be fully transparent about the limitations of any technology, and compel them to release any requested scientific data relating to the claimed reliability and validity of technology.

Dr Christopher Lawless
1 November 2019

\textsuperscript{26} Big Brother Watch (2018).
\textsuperscript{27} Wang & Kosinski 2018; Purshouse & Campbell 2019.
List of References


