INTRODUCTION

1. Liberty welcomes the opportunity to respond to the Justice Sub-Committee on Policing’s consultation on police use of facial recognition in Scotland, and in particular the equalities and human rights implications of the use of this technology.¹

2. Facial recognition technology can either be ‘live’ or ‘retrospective’. Police Scotland has advised that it is already using retrospective facial recognition from recorded CCTV by matching against faces in the UK-wide Police National Database [PND], but it is awaiting the appointment of the Biometrics Commissioner before trialling live facial recognition.²

3. There are references to the use of facial recognition in Police Scotland’s document “Policing 2026: Our 10 year strategy for policing in Scotland”.³ The references in the strategy are not detailed, and simply indicate a desire to use the technology to identify suspects. There is no specific reference to facial recognition contained in either the corresponding implementation plan⁴ or three

¹ Liberty does not specifically comment on the remaining consultation questions, which include the type of facial recognition technology used by the police service, the circumstances in which equipment is used to capture images or Police Scotland’s purposes in considering the use of such technology. However, in discussing the rights impact of this technology, we draw upon existing practice of police use of facial recognition outside Scotland.

² Logan (2019), "On our way to a Big Brother society": MSPs urged to ban facial recognition cameras, Commonspace, 7 October 2019, Available at: https://www.commonspace.scot/articles/14781/our-way-big-brother-society-msps-urged-ban-facial-recognition-cameras


year financial plan. Police Scotland recently wrote to the Sub-Committee indicating that facial recognition is part of the wider suite of current and developing biometric technologies that it has an ambition to explore, although they confirmed their intention to await the developments in the passage of the Scottish Biometrics Commissioner Bill.

4. This consultation response deals first with the potential introduction of live facial recognition by Police Scotland and then with retrospective live facial recognition.

5. It is a matter of grave concern that the Equality and Human Rights Impact Assessment (EqHRIA) carried out in relation to the strategy concluded that “Human Rights Impact Assessment Analysis of the Strategy…identified no potential infringements to any of the rights”, despite specific references to the introduction of facial recognition. This suggests that the significant rights issues presented by the introduction of such biometric surveillance technologies are, wilfully or otherwise, being ignored.

LIVE FACIAL RECOGNITION

6. Live facial recognition systems take the biometric data of every person who passes the camera – creating a unique facial map which is matched against those on a “watch list”. The scanning and checking of a person’s identity takes place without their consent, and often without their knowledge. UK police have used this indiscriminate surveillance on our streets and in shopping centres, around stadiums and concert venues – it has even been used to surveil people attending peaceful protests.

7. The police-curated watch lists which have been used by forces thus far are shrouded in secrecy. There is no specific regulation as to who can be placed on a watch list, or what sources can be used. Documents produced in the course of the litigation against South Wales Police (SWP) confirmed that anyone could be included on a watch list – including people who are not wanted

---

6 Scottish Parliament Justice Sub-Committee on Policing (2019), Facial Recognition: how policing in Scotland makes use of this technology - Call for Evidence, 4 October 2019, Available at: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/113104.aspx
7 Ibid
11 Concerts have included Kasabian (December 2017), Liam Gallagher (December 2017), Stereophonics (March 2018), Beyoncé (June 2018), Rolling Stones (June 2018), Ed Sheeran (four concerts in June 2018). See: Deployments section, http://afr.south-wales.police.uk/
12 Goulding (2018), The police’s use of facial recognition technology will affect our daily freedoms, 10 August 2018, Metro, Available at: https://metro.co.uk/2018/08/10/the-polices-use-of-facial-recognition-technology-will-affect-our-daily-freedoms-7822753/
by the police or the courts.\textsuperscript{13} The Met used facial recognition to monitor people at Remembrance Sunday in 2017, and aimed to exclude people from a public remembrance event on the basis that they had a mental health condition.\textsuperscript{14} Watch lists may also include images obtained from social media.\textsuperscript{15} The Office of the Information Commissioner, in giving evidence to the Science and Technology Committee, stated that:

“custody images will be used to form the basis of ‘watchlists’ which are then used when automatic facial recognition technology (AFR) is utilised by police forces in public spaces. The Commissioner is so concerned with the practices in some areas that a priority investigation has been opened to understand and investigate the use of AFR by law enforcement bodies in public spaces.” \textsuperscript{16}

8. Unlike other biometric systems utilised by law enforcement, such as fingerprinting, facial recognition can be used for passive and general surveillance and does not require the knowledge, consent or active participation of the people being monitored.

THE RISK TO OUR PRIVACY

9. The Human Rights Act 1998 (“HRA”) gives effect in domestic law to the European Convention on Human Rights (ECHR). Article 8 ECHR requires that any interference with the right to a private life is in accordance with law, and is both a necessary and proportionate means for achieving a legitimate aim. In Liberty’s view, the use of facial recognition in public spaces fails to meet these thresholds. To the extent that it involves indiscriminately scanning, mapping and checking the identity of every person within the camera’s range – using their deeply sensitive biometric data – it is an enormous interference with the right to privacy.

10. While facial recognition has a significant privacy impact when it works, it also has a significant privacy impact when it does not. A “false match” occurs where someone is stopped following a facial recognition match but is not, in fact, the person included on the watch list. In the event of a false match, a person attempting to go about their everyday life is subject to an invasive stop and may be required to show identification, account for themselves and even searched under other police powers. Liberty has observed a distinct lack of human


oversight over live matches and has significant concerns about decisions of this nature being influenced by complex and impenetrable technology.

11. The privacy concerns examined throughout this briefing cannot be addressed simply by requiring the police to delete images captured of passers-by, or by improving the accuracy of the technology. Inaccurate facial recognition results in a high rate of false stops and corresponding rights infringements. However, accurate facial recognition will simply help ensure that everyone’s privacy rights are equally infringed.

THE RISK TO OUR FREEDOM OF EXPRESSION AND ASSOCIATION

12. The ECHR requires that any interference with the Article 10 right to free expression, or Article 11 right to free association, is in accordance with law, and both necessary and proportionate. The use of facial recognition technology can be highly intimidating. If we know our faces are being scanned by police and that we are being monitored when using public spaces, we are more likely to change our behaviour. Those changes in behaviour may relate to where we go and who we choose to associate with. For a whole host of reasons linked to a desire to retain our anonymity and to keep our activities and political views private, we may decide not to attend public meetings, to avoid our local high street, or change who we spend time with in public spaces. For example, Liberty has worked with protesters who expressed how intimidating they found the presence of facial recognition at demonstrations, and who said that they would be reluctant to attend a future protest where it was in use. Even where images or biometric data are not retained following a deployment of facial recognition, this technology could still be used to identify and record that a known person was at an event.

13. If facial recognition interacts with other surveillance technologies, people are increasingly likely to feel they have no choice but to avoid expressing religious or dissenting political views in public, and may consequently avoid attending demonstrations, political meetings or places of worship. As a society, this will undermine our ability to express ideas and opinions, communicate with others and engage in democratic processes, as people increasingly choose not to pay the price of handing over their sensitive biometric data in order to do so.

17 Liberty observers witnessed the stop of a man following a false match at a Met deployment. There was no observable human verification process to assess the match before the man was stopped. See Couchman (2018), “Not A Fool-Proof System”: Facial Recognition In Action [Blog], 29 June 2018, Available at: https://www.libertyhumanrights.org.uk/news/blog/%E2%80%9Cnot-fool-proof-system%E2%80%9D-facial-recognition-action

18 Studies have shown that people were less inclined to attend mosques they thought were under government surveillance. Business owners muted political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook. See: Shamas et al (2103), Mapping Muslims: NYPD Spying and its Impact on American Muslims, Muslim American Civil Liberties Coalition (MACLC), and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, Available at: http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

19 The European Court of Human Rights has held that the UK violated the right to privacy of Mr John Catt, a peace movement activist who – despite having never being convicted of any offence – had his name and personal data included in a police database and was subject to intrusive surveillance.
THE RISK TO OUR FREEDOM FROM DISCRIMINATION

14. Article 14 ECHR ensures that no one is denied their rights because of their gender, age, race, religion or beliefs, sexual orientation, disability or any other characteristic.

15. Liberty has raised concerns regarding the racial and socio-economic dimensions of police trial deployments thus far. For example, the Met has deployed facial recognition at Notting Hill Carnival, a festival celebrating Caribbean culture in the UK, for two years running, as well as twice in the London Borough of Newham. Newham is one of the UK’s most ethnically diverse places and the white British population stands at 16.7%, the lowest in the UK. The Office of the Information Commissioner also noted to the Science and Technology Committee that:

“The Committee’s view was that facial recognition technology should not generally be deployed, beyond the current pilots, until the current concerns over the technology’s effectiveness and potential bias have been fully resolved. The Commissioner is concerned that this has not been fully addressed and it is not yet clear how the ‘oversight board’ will address these issues.”

16. Studies have shown facial recognition technology disproportionately misidentifies people of colour, trans people, young people and women – meaning that people from these groups are more likely to be wrongly stopped and questioned by police, and to have their images retained as the result of a false match. The same conclusion was reached in a study conducted by the FBI. While the causes of discrimination within algorithms can vary, in this case it is likely to stem from the fact that, when an algorithm is trained to recognise human faces using training data sets, it is exposed to an insufficiently diverse set of images. The disproportionate use of this technology in communities against which it underperforms (according to its proponents’ standards) is deeply concerning.

17. However, Liberty notes that improving the accuracy of this technology only serves to increase the pervasiveness of the rights infringements associated with facial recognition. As Dr Julia Powles points out,

“even apparent success in tackling bias can have perverse consequences. Take the example of a facial recognition system that works poorly on women of color because of the group’s underrepresentation both in the training data and among system

---


designers. Alleviating this problem by seeking to “equalize” representation merely co-
cepts designers in perfecting vast instruments of surveillance and classification.”

18. The EqHRIA carried out with regard to the aforementioned “Policing 2026”
strategy concluded that:

“analysis of the strategy, from an equality perspective, appears to support that the
proposed changes will have no direct or indirect adverse or disproportionate impact
on protected groups in the wider community or in respect of partnerships”.
Police Scotland are required, under their public sector equality duty24, to have due
regard to three matters: (a) the need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the 2010 Act; (b) the
need to advance equality of opportunity between persons who share a relevant
protected characteristic and persons who do not share it; and (c) the need to foster
good relations between persons who share a relevant protected characteristic and
persons who do not share it. The analysis undertaken as part of the EqHRIA appears
to fall short of this standard, neglecting to consider the evidence outlined above as to
discriminatory outcomes which will be perpetuated by the tool.

THE FUTURE OF MASS SURVEILLANCE

19. The ubiquity of surveillance cameras, which can be retrofitted with facial
recognition software and fed into police databases, means that there is already
an apparatus in place for large-scale intrusive surveillance, which could easily
be augmented by the widespread adoption of facial recognition technology. Use
of facial recognition technology in the private sector could also result in the
build-up of large repositories of photographs or the associated biometric data,
which could be requested by police for law enforcement purposes.

20. There have also been concerning developments in use of police data by private
companies. In October 2018, it was revealed that the Trafford Centre in
Manchester had scanned the face of every visitor for a six-month period –
approximately 15 million people25 – and matched them against a watch list
provided by Greater Manchester Police.26 Recent reports also revealed that live
facial recognition was being used at the privately-owned but publicly-accessible
site around King’s Cross station, and that both the Met and British Transport
Police had provided images for their use – despite originally denying doing so.27
The Surveillance Camera Commissioner has noted the dangers of private
companies utilising police data in this way.28

23 Powles (2018), The Seductive Diversion of ‘Solving’ Bias in Artificial Intelligence, Medium, 7 December 2018, Available at: https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53
24 See section 149(1) of the Equality Act 2010
25 Robson and Koncienzcy (2018), How to find out if you were one of the 15 MILLION caught in a secret surveillance pilot, Liverpool Echo, 15 October 2018, Available at: https://www.liverpoolecho.co.uk/news/liverpool-news/how-find-out-you-were-15284099
26 Robson (2018), Greater Manchester Police monitored every visitor to Trafford Centre for SIX MONTHS using controversial technology until they were told to stop, Manchester Evening News, 14 October 2018, Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943
27 BBC (2019), Met Police gave images for King's Cross facial recognition, 6 September 2019, Available at: https://www.bbc.co.uk/news/technology-49586582
21. The risks presented by continued expansion of facial recognition include the use of this technology through the pre-existing CCTV network and body-worn video, enabling passive, real-time monitoring of us all. Police forces have made known their plans to make this technology “portable” through digital Samsung Galaxy devices,29 as well as recognising the potential for it to be used in conjunction with police body worn video and CCTV.30

RETROSPECTIVE FACIAL RECOGNITION

22. Retrospective facial recognition is currently in use by Police Scotland. Police Scotland has advised the Sub-Committee that this involves matching against faces in the UK-wide PND – but Liberty notes that other police forces have accepted that images for facial recognition matching could be taken from elsewhere, including social media.31

23. The privacy infringements presented by retrospective use of facial recognition are not dependent on the presence of a police facial recognition van or a complicated ad-hoc set-up but can make use of footage from a vast and existing surveillance infrastructure – including CCTV cameras and social media. As outlined above, being aware of the potential for such technologies to identify and track us may lead to self-censorship and a shift in the way we perceive, engage with and behave in public spaces – with enormous implications for our democratic values.

24. While retrospective facial recognition can be used to identify a single individual, it can also be used to search a feed of CCTV for a particular person. In this way, retrospective use can still involve the indiscriminate scanning, mapping and identity checking of every person who appears in a section of CCTV footage.

25. The PND contains approximately 23 million images32 of which around 10 million are technically suitable facial images of sufficient quality to be searchable.33 Images in the database are not limited to those who have been arrested, charged or convicted of an offence. The legality of the retention of custody images was challenged and in a 2012 judgment the High Court held that the continued retention of images from individuals who had not been convicted was unlawful without case by case consideration.34 The Home Office responded to this judgment by publishing, five years after the judgment was handed down, a Review of the Use and Retention of Custody Images.35 The Review reiterated

---

30 Ibid
32 This includes images of marks, scars, tattoos and some low-quality images that cannot be searched, bringing the actual number of custody images down to around 15 million.
33 Around 15 million of the images are technically searchable but only around 10 million can actually be searched and give a useable result. Figures provided by Home Office Digital, Data and Technology
34 31R(RMC and F) v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin)
that the time periods for review of information about an arrestee as set out in the principles of management of police information\textsuperscript{36}, depending on the offence, should be applied specifically to custody images. Additionally, the Review introduced a right for an arrestee to make a request to a Chief Officer for their facial image to be deleted, with a presumption of deletion in certain, limited circumstances.

26. The Minister of State for Countering Extremism confirmed, in evidence to the House of Commons Science and Technology Select Committee on 6 February 2018, that one of the reasons why the Home Office had not proposed automatic weeding of custody images, particularly those on the PND, was that it was not technically possible.\textsuperscript{37} The PND is therefore plainly inappropriate for use in conjunction with facial recognition.

CONCLUSION

27. The breadth of public concern around this issue is clear. At the time of writing, Liberty’s petition calling for a ban against the use of facial recognition in publicly accessible places had over 10,000 signatories, and a statement released in September 2019 by Big Brother Watch was signed by politicians from across the political spectrum and 25 race equality and technology campaign groups – as well as technology academics and legal experts.\textsuperscript{38} Introducing legislation or other frameworks to regulate the use of this authoritarian surveillance tool will not address rights concerns and is permissive of a disproportionate surveillance regime in which we are increasingly tracked and monitored, and in ways felt most keenly by communities already experiencing over-surveillance.

Liberty
31 October 2019

\textsuperscript{36} The principles of management of police information (MoPI), Available at https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

\textsuperscript{37} Baroness Williams of Trafford, the Minister of State for Countering Extremism, gave evidence to the House of Commons Science and Technology Select Committee on 6 February 2018, followed up by a letter dated 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf