

## JUSTICE SUB-COMMITTEE ON POLICING

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

#### WRITTEN SUBMISSION FROM DR BIRGIT SCHIPPERS, ST MARY'S UNIVERSITY COLLEGE BELFAST

I would like to thank the Justice Sub-Committee for the opportunity to respond to the call for evidence on the use of facial recognition technology (FRT) by Police Scotland. This response draws on my work as a political theorist researching the ethics and politics of artificial intelligence (AI)-based technologies, with particular reference to the human rights aspects of biometric technologies, such as FRT. I will address four areas, which focus on the potential impact of police use of FRT on rights-based, democratic societies.

#### 1. Bias and discrimination

FRT analyses facial images, which are matched against images in already existing databases. Despite improvements in the precision of this technology, there remain significant concerns over its accuracy rates, which are lower when analysing darker-skinned and female faces. This 'white guy bias',<sup>1</sup> which stems primarily from the predominantly white and male images that populate the data training sets used to develop FRT, is compounded for darker-skinned women.

Concerns over the accuracy rate of FRT have been documented by academic researchers<sup>2</sup> and civil liberties organisations,<sup>3</sup> especially by those working in the United States. Given the current state of this technology, its deployment in police operations, for example when making arrests or in the policing of public events, has potentially discriminatory effects. It would be hasty and ill-considered for any police force to use a technology that produces biased outcomes, and whose efficacy and accuracy remains an issue of concern. The discriminatory effects of FRT could undermine trust in the fairness of policing, and would leave the police vulnerable to accusations of bias and discrimination, especially in their relationship with BAME communities.

Equally serious are concerns over automation bias with respect to machine-generated decisions. Despite assurances, given for example by the Scottish Police Federation in its submission to this call for evidence, that FRT will be treated as intelligence and thus subject to human checks and verification, there is a real worry that machine-generated outcomes, whether with or without human oversight, will determine how

---

<sup>1</sup> K. Crawford. 2016. 'Artificial Intelligence's White Guy Problem.' <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html>.

<sup>2</sup> J. Buolamwini and T. Gebru. 2018. 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.' *Proceedings of Machine Learning Research* 81: 1-15.

<sup>3</sup> J. Snow. 2018. 'Amazon's face recognition falsely matched 28 members of Congress with mugshots.' <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.

agencies such as the police treat the public, and in particular individuals from minority ethnic backgrounds. A recent survey conducted by the London Policing Ethics Panel indicates that BAME communities have higher than average levels of mistrust in the use of this technology, especially when deployed by the police; there is a real risk that adopting this technology will further increase the levels of mistrust.<sup>4</sup>

## 2. Right to privacy

FRT has been described as a ‘menace disguised as a gift’,<sup>5</sup> and as a ‘solution in search of a problem.’<sup>6</sup> It is a blunt instrument that enables the automated and indiscriminate live surveillance of people as they go about their daily business, giving authorities the chance to track our every move. There are legitimate worries with respect to its intrusive nature, in particular its impact on the right to privacy, which remains a cornerstone of every liberal society. When linked to the already expansive network of CCTV cameras that exists within the UK, FRT will bring surveillance to a new level; its use by law enforcement agencies, such as the police, will have a potentially corrosive impact on our civil liberties and human rights.

The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. FRT’s indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it.<sup>7</sup>

A commonly expressed human rights principle is that surveillance should be necessary and proportionate.<sup>8</sup> This means surveillance should be restricted to the pursuit of serious crime instead of enabling the unjustified interference into our liberty and fundamental rights. FRT has the tools to bypass the criteria for necessity and proportionality, providing the technical capacity for blanket and round-the-clock surveillance. It is a technology of control that is symptomatic of a mistrust of citizens.

Whilst FRT can be used for blanket surveillance, it can also be deployed selectively, for example to identify migrants and refugees, or to target already marginalised individuals and communities. The use of handheld mobile devices with a facial

---

<sup>4</sup> London Policing Ethics Panel. 2019. *Final Report on Live Facial Recognition*. [http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr\\_final\\_report\\_-\\_may\\_2019.pdf](http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf).

<sup>5</sup> W. Hartzog and E. Selinger. 2018. ‘Facial recognition is the perfect tool for oppression.’ <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

<sup>6</sup> W. Wiewiórowski. 2019. ‘Facial recognition: a solution in search of a problem?’ [https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem\\_en](https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en).

<sup>7</sup> ICO. 2019. ‘Statement: Live facial recognition technology in King’s Cross.’ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross>.

<sup>8</sup> Article 19. 2017. ‘UN resolution affirms surveillance that is not necessary or proportionate is against the right to privacy.’ <https://www.article19.org/resources/un-resolution-affirms-surveillance-that-is-not-necessary-or-proportionate-is-against-the-right-to-privacy/>. See also ICO.

recognition app by police forces raises the spectre of enhanced racial profiling at the street level.<sup>9</sup>

### **3. Democracy**

The human rights implications of FRT use by police forces extend beyond the threat to the right to privacy; FRT has consequences for our rights as citizens in democratic societies. Blanket surveillance facilitated by FRT can deter individuals from attending public events. It can stifle participation in political protests and campaigns for social and political change, and it can discourage nonconformist behaviour. This chilling effect is a serious infringement on the right to freedom of assembly, association, and expression.

A recent report by the Information Commissioner's Office (ICO) has criticised a lack of detailed and specific information on where and when live FRT is processing facial data in real time.<sup>10</sup> As citizens, we do not have the opportunity to consent to the recording, analysing and storing of our images in databases, and we are denied choice and control over the use of our own images. In addition to concerns over a possible lawful use of FRT by the police and the negative impact this has on democracy and human rights, we should also be concerned about the troubling capacity for abuse, especially in light of the growing sophistication of deep fakes.

### **4. Data sharing and data security**

Public-private collaborations in policy areas as sensitive as policing blur the boundaries between the role and responsibilities of the police, and the interests of private corporations. Recent evidence from the United States attests to the close relationship between the business interests of private corporations that develop and sell FRT, for example Amazon, and its use by state agencies, such as the controversial US Immigration and Customs Enforcement (ICE), which has been heavily criticised for its tactics in dealing with migrants. Police Scotland's ten-year strategy *2026: Serving a Changing Scotland*, alludes to the prospect of such sharing of facial images between private corporations and the police in its Castle Shopping Centre scenario: this scenario outlines the application of FRT to images captured via CCTV. The likelihood of partnering with what it terms '3<sup>rd</sup> party contractors' is also confirmed by the Scottish Police Federation in its submission to this call.

These collaborations raise particular concerns with respect to the sharing of our facial images; the creation of, and access to, image databases, or watch lists; and the security of our biometric data, and their vulnerability to the actions of hackers. They raise the prospect that private companies and law enforcement agencies are sharing our images to build watch lists of potential suspects without our knowledge or consent. This is a serious threat to our individual rights and civil liberties.

---

<sup>9</sup> BBC News. 2019. 'South Wales Police to use facial recognition app on phones.' <https://www.bbc.co.uk/news/uk-wales-49261763>.

<sup>10</sup> ICO. 2019. ICO investigation into how the police use facial recognition technology in public places. <https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf>.

In light of these concerns about facial recognition technology, we need a more prominent conversation on its impact on our rights and civil liberties. Without proper and effective regulation of FRT use, we risk creating a dystopian police state in what was once a free, democratic country.

**Recommendations:**

1. There should be a moratorium on the deployment of FRT by Police Scotland until there is sufficient and independently verifiable evidence that this technology is fully compliant with the full suite of national and international human rights and equality obligations and standards. This moratorium should take cognisance of the Automated Facial Recognition Technology (Moratorium and Review) Act 2019.
2. FRT should be subject to an effective governance framework that includes legal and democratic accountability, and that operates at local and national levels.
3. FRT's wide-ranging impact on the principles and practices of democratic politics requires a much more prominent and wide-ranging conversation than is currently taking place. Individuals and communities must be educated on FRT and its ethical and political challenges. The Scottish Parliament's Justice Sub-Committee, together with the Scottish Parliament, should initiate such a public debate on the use of FRT by Police Scotland in the wake of this call for evidence. This debate must include key stakeholders, including human rights and civil liberties organisations, and it should be pro-active in facilitating the involvement of the broadest possible range of participants.

Dr Birgit Schippers  
13 November 2019