1. Thank you for the opportunity to make a submission to the Sub-Committee’s Inquiry considering how policing in Scotland makes use of facial recognition technology, and whether any such use is lawful, ethical, proportionate and transparent.

2. We make this submission based on our research expertise. We have published numerous peer-reviewed academic articles on the regulation of forensic and biometric technologies, looking in particular at the human rights implications of these technologies when they are used in a policing context. We have written on the regulation of facial recognition technology (FRT),¹ and are currently working on a research project in this area, funded by the New Zealand Law Foundation.

3. Here, we highlight some of the particular concerns linked with the use of facial recognition technology in Scotland and make recommendations about its future use.

Executive Summary
- Any use of facial recognition searching on the UK Police National Database may violate human rights laws, and has particularly serious implications for non-convicted persons, whose images are retained on that database.
- The use of facial recognition technology in public spaces and at major events has been controversial in other jurisdictions, and raises unique human rights and data protection issues.
- The legal basis for regulating facial recognition technology in certain environments is too broad to regulate the interferences with fundamental human rights occasioned by FRT.

Facial Recognition Surveillance: Human Rights Implications

4. Whilst the use of FRT might bring considerable benefits in some circumstances, its increasing use has raised concerns. Some of these concerns are instrumental. For example, FRT may not truly achieve public safety benefits.

5. Instrumental concerns also relate to the accuracy of the technology itself. The performance of FRT is not easily measured as technological systems and algorithms vary depending on the task they are performing, and how ‘success’ is

defined. For example, an FRT system may be set at a particularly low accuracy threshold to maximise the number of identifications (with full awareness that this will also increase the number of false positive matches). Some of the concerns raised over the accuracy of FRT surveillance are well founded. The performance of FRT systems can vary relative to the gender, ethnicity and age of individuals targeted, which raises concerns that FRT will manufacture, and reinforce any latent, police discrimination against minority groups.

6. FRT might also have a detrimental impact on fundamental human rights. When FRT is deployed a number of human rights might be impacted. These includes but are not limited to privacy, freedom of speech and freedom from discrimination. The particular constellation of human rights impacts will vary depending on the features of the particular FRT system that is used, the context in which it is used, the manner of this use, the safeguards that are in place to regulate a particular deployment and other factors.

7. Like fingerprint scanning and DNA profiling, FRT involves the processing of biometric information about the individual. The technology allows the police to go much further in monitoring individuals as they occupy public space than ordinary/human observation would. The FRT process ‘involves the creation of informational equivalents of body parts that exist outside their owner and are used and controlled by others.’ In September 2019, a Divisional Court in R (Bridges) v Chief Constable of South Wales Police held that the use of FRT to scan the claimant as he traversed public space engaged his right to respect for private life under Article 8(1) of the European Convention on Human Rights (ECHR).

8. FRT may have a ‘chilling effect’ on public assemblies, freedom of expression, and the general use of public space by certain communities and demographics. Overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources. These findings, which are supported by empirical research from the United States, suggest that the presence of visible surveillance at meetings and other political gatherings will reduce perceptions of legitimacy, and harm the efforts of such groups to be taken seriously and attract support from

---

their target audiences. Furthermore, the perception of being controlled in the public space breaks down the trust in police and other state institutions.⁸

**Facial Image Searching on the Police National Database**

9. The Police National Database is available to all police forces in the United Kingdom, allowing forces to share intelligence including custody images across all jurisdictions in the UK. Given that facial images form part of the individual’s private life, it is crucial that these images are not retained by police for longer than is necessary. The Scottish approach of uploading custody images to the Police National Database only after a charge, and deleting images six months after proceedings have concluded without a conviction, is welcomed and should be maintained. However, additional safeguards may be needed if Scottish police forces are to use automated facial recognition software on this database. The mere storage of custody images on this database raises privacy and data protection considerations, and the use of facial recognition software is likely to exacerbate any privacy issues as this involves biometric data processing. Moreover, whilst Scottish practices on uploading images to the Police National Database may well safeguard the rights of non-convicted persons in Scotland, any use of facial recognition software on the database by police in Scotland may engage the rights of non-convicted persons, as their images have been uploaded and retained on the database by forces from other jurisdictions.

10. In its report, the House of Commons Science and Technology Committee recommended that the Government should introduce a “fully automatic image deletion system for those who are not convicted” and that, if there is any delay in implementing such a system, the Government “should move to introduce a manually processed comprehensive deletion system as a matter of urgency.”⁹ We could find no evidence that the Government has begun a process of automatic or comprehensive manual deletion of this data. In its Biometrics Strategy, the Home Office suggested that its new Law Enforcement Data Service would, in theory, “enable more efficient review and where appropriate, automatic deletion of custody images”.¹⁰ However, it made no commitment to implement any such system of automatic deletion, or to develop new policies or rules governing the retention of custody images taken of non-convicted persons.

---

⁸ Blake Schmidt “Hong Kong Police Already Have AI Tech That Can Recognise Faces” Bloomberg (23 October 2019).
Regulating the Police Use of Facial Recognition Technology

11. The United Kingdom has been at the vanguard of the use of FRT, with South Wales Police, the London Metropolitan Police, and various quasi-private schemes using it for policing and security purposes for a number of years. This is despite “the lack of a clear legislative framework for the technology”.

12. The United Kingdom has not introduced any specific laws relating to FRT; this situation has prompted much commentary as well as an ongoing legal challenge. A number of academic commentators, including some of this paper’s authors, suggested that police deployment of FRT in England and Wales may be held unlawful due to the absence of domestic legal authorisation. Moreover, the Law Society for England & Wales suggested that it is highly unclear whether facial recognition at scale can meet a test of strict necessity as required under the Data Protection Act 2018 (DPA 2018), particularly given issues of accuracy and its “highly unproven nature”. The legal basis regulating the use of the technology lies in the DPA 2018, along with the Regulation of Investigatory Powers (Scotland) Act 2000; the National Strategy for Public Space CCTV; and relevant human rights and common law principles. This framework is implicit and overlapping, in that it does not set out specific principles and rules for the use of FRT.

13. In the Bridges case, the Administrative Court in Wales held that this implicit framework was sufficiently precise to be considered ‘in accordance with the law’ under Article 8(2) ECHR. However, this finding is controversial, going against the balance of legal commentary on the use of FRT in England and Wales. It may soon be overturned on appeal. We note that the trials of live facial recognition in England and Wales were marred by troubling police practices and inconsistent approaches between trialling forces, which suggest that the legal framework underpinning these trials was insufficiently narrow to adequately regulate the operations of FRT in a live public space surveillance context.

Recommendations

14. We recommend the following should precede any roll out of FRT by Police Scotland:

https://www.met.police.uk/live-facial-recognition-trial/
Dan Sabbagh “Facial recognition technology scrapped at King's Cross site” The Guardian (2 September 2019).
- Notwithstanding the outcome of *Bridges*, we recommend that FRT should not be deployed in a policing context until concerns over the technology’s effectiveness and potential bias have been confronted and mitigated by requiring transparency of algorithms, robust oversight, and limited use.
- We recommend a moratorium until statutory provisions specifically regulating the use of FRT have been introduced and an oversight and evaluation system has been established.
- We suggest that respect for human rights must guide the use of FRT. Transparency of use and procedure is key. In relation to policing, FRT’s use must be necessary in terms of the policing aim and operation, rather than being driven by the mere existence or appeal of the technology.
- A single regulatory body should be established to oversee the use of FRT.

We would be pleased to provide further information on any of the points mentioned above.

Yours faithfully,

Dr Joe Purshouse, University of East Anglia
Professor Liz Campbell, Monash University
Dr Marcin Betkier, Victoria University of Wellington
Dr Nessa Lynch, Victoria University of Wellington

28 October 2019