I am pleased to have the opportunity to make a submission to the Scottish Parliament Justice Sub-Committee on Policing Inquiry into Facial Recognition. I am a legal academic, who recently returned to Scotland to work at Strathclyde Law School. My expertise is in the regulation of new digital technologies and I have been conducting research on the ethical and legal dimensions of facial recognition technology and its interaction with human rights, including privacy. It is from this perspective that I make this submission. Please do not hesitate to contact me if you require any further information or clarification.

Overall, given the deficiencies of facial recognition technology, the intrusive ways in which facial recognition technology is already being used to monitor indiscriminately the general public (and not only those suspected of a crime) and the less-than-ethical conditions in which facial recognition technology is being researched and developed, I urge the Committee to become an international leader in ethical technology policy by recommending a moratorium on the use of facial recognition technology in Scotland, especially by police forces.

1. Deficiencies of facial recognition
There are concerns about the ways in which facial recognition technologies are deficient and inaccurate, particularly regarding the technology’s inbuilt biases via datasets on which it is trained. In particular, facial recognition technology may exhibit sexist and racist biases in its misidentification of faces (see for instance how black women’s faces were misidentified by one particular product).¹ The implications of inaccurate facial recognition may entail that innocent people are misidentified as suspects or perpetrators and given the sexist and racist biases, this may disproportionately affect black women the most, with white women and black men also affected. This lack of accurate identification, and the consequences for misidentification of innocent people (‘false positives’) in the policing context, with a particular impact on Black and Minority Ethnic people and women (with BAME women particularly affected) should raise red flags about the discriminatory impact of facial recognition use by police and the possibility or even likelihood of innocent people being misidentified by such systems.

2. Mass-monitoring of the public
The ways in which facial recognition is being deployed in public places in other parts of the UK involves indiscriminate monitoring of all members of the public in a

particular area. This has been the case with the controversial trials of facial recognition at large sporting and music events and the Notting Hill Carnival in London (although this was suspended in 2018 after a report from NGO Big Brother Watch which found the product used by the Metropolitan Police had a 98% false positive rate). Other trials in London have met with public resistance, including people covering their faces (with at least one person being fined for doing so). This suggests a lack of social licence for the police to roll out facial recognition in public area which indiscriminately captures data from all persons in the vicinity.

A recent challenge to the South Wales Police’s use of facial recognition on the basis of data protection and human rights infringements has been unsuccessful before the High Court of England and Wales, although the decision in the process of being appealed. Since this decision, the UK Information Commissioner’s Office (ICO) has issued an Opinion on police use of facial recognition in public, expressing concern about human rights and data protection impacts of facial recognition and calling for a statutory code of practice governing how the police should use this technology.

Earlier this year, the Californian City of San Francisco voted to ban facial recognition technology from being used by the police force and other local public agencies due to the technology’s unreliability and its invasion of privacy and civil liberties. Since San Francisco’s example, there have been calls for a global moratorium on facial recognition technology for mass surveillance purposes, led by civil society groups and concerned individuals (including myself).

I urge the Committee to consider deeply the impact on the privacy and other human rights of the general public in being subjected to invasive mass-monitoring by facial recognition technology used by police, the lack of social licence with which facial recognition has been deployed so far, and the example of other cities and regions internationally such as San Francisco which has prohibited the use of facial recognition technology altogether by public agencies. I do not believe that the ICO’s call for a statutory code will be sufficient to allay these concerns.

---


A further point of concern is the circumstances in which facial recognition technology is being researched and developed. Concerns have been raised about the lack of diversity in researchers and developers making facial recognition technology in US tech firms (who are mainly white men), which may be one reason why the products also exhibit racial and gender biases.8

A significant amount of facial recognition is also being developed by China’s growing technology industry, some of which is being created and trialled in the ‘laboratory’ of Xinjiang/East Turkestan where minority populations including Uyghurs and other groups have been subject to severe repression and human rights violations by the Chinese government.9 It has been reported that companies including Hikvision, Taisau, SenseTime and Megvii have provided facial recognition technology which is or was used in Chinese government surveillance in Xinjiang, and some of these companies have recently been placed on a US government trade blacklist.10 Yet, products and services developed in China have started to be exported to other countries, including by companies which have been active in providing surveillance technology and facial recognition capabilities in Xinjiang. Such recipient countries include Ecuador (with its notable ECU-911 system), Zimbabwe, Pakistan and Germany.11

The development of facial recognition technology in highly unethical environments such as Xinjiang should provide another reason why facial recognition overall is an unethical technology with worrying human rights implications from its conception, development and deployment. Even facial recognition technology developed in other countries such as the US is not being ethical in conditions.

In conclusion, due to the deficiencies of facial recognition technology, the invasion of human rights and civil liberties its deployment in public places entails and the unethical conditions in which many facial recognition products and services are researched and developed, I urge the Committee to listen to the international calls for a moratorium on facial recognition’s use especially

8 Tessa Townend, ‘Most engineers are white — and so are the faces they use to train software’ (Recode, 18 January 2017) https://www.vox.com/2017/1/18/14304964/data-facial-recognition-trouble-recognizing-black-white-faces-diversity
10 Mariella Moon, ‘US government adds Chinese facial recognition firms to entity list’ Engadget 7 October 2019) https://www.engadget.com/2019/10/07/us-entity-list-chinese-facial-recognition-video-surveillance/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS91cmw_c2E9dCZyY3QaIZxPSZlc3JjPXMMC291cmNIPxldyY2JIDOymNhZD1yamEmdWFjdD04JnZID0yyYWhMoy5a3b5UDdldj0ub1ubEfoVUtRVVBBSFzTEJcd1FGakF2zrR5USFQULmdXJsPWhdH8zJTBNB6JGJtJGd3d3LmVuz2FkZZV0LmNvbSUyRjIwMTkMlMkYxMCUyRjA3J
by law enforcement, and take a leading role in developing ethical technology policy by recommending that facial recognition technology be banned from use by Scottish police forces and other public agencies.

Dr Angela Daly
Senior Lecturer, Centre for Internet Law & Policy, Strathclyde Law School
1 November 2019