The Scottish Human Rights Commission (the “Commission”) welcomes the intervention of the Justice Committee in addressing this issue and would welcome the opportunity to present evidence before the Committee. We are aware the Committee is currently scrutinising the Scottish Biometrics Commissioner’s Bill and has previously heard evidence on the Police Scotland introduction of digital device triage Systems (‘cyber-kiosks’). The Committee is therefore live to concerns over the human rights impacts of new and developing technologies particularly in relation to their role in policing and public security. The current issue inhabits a similar legal context and there are broadly similar themes to the Commission’s views as previously expressed. The Commission does not propose to repeat the detailed reasoning and analysis set out in previous submissions, but wishes to draw your attention to the key thematic points relevant to the current issue.

1. **The type of facial recognition technology used by the police service, the circumstances, and any implications.** For example, Police Scotland accessing facial recognition images from CCTV cameras, national databases, body worn video cameras, and potentially mobile phones: The Independent Advisory Group (IAG) on the Use of Biometric Data in Scotland defined biometrics as ‘any physical, biological, physiological or behavioural data, derived from human subjects, which have the potential to identify an individual.’. In this context the Commission’s submission regarding biometrics, particularly our desire for a Statutory Code of Conduct is of relevance. There is currently no adequate legal framework governing the capture, storage and use of biometric data in the way that Police Scotland operationally deploy law enforcement. The IAG report specifically identified image data (p8) as being within the review’s remit. For brevity’s sake, it is assumed that the Justice Committee is familiar with the IAG report as well as our submissions on the Bill. It would be helpful if the Committee would consider Section 4 of the IAG report which contains the Commission’s analysis of the current legal framework. The Committee will note at paragraph 4.9 that facial images are cited as an area where there is a lack of evidence of the effectiveness/reliability of biometric related technologies. We note that the Law Society of Scotland addresses this issue in detail in their submission and share their concerns regarding the use of this technology.

2. **The circumstances in which equipment is used to capture images, for example the use of body worn video cameras at major events, such as protests and football matches:** The widespread use of image capture and the potential use of live facial recognition all engage Article 8 of the European Convention on Human Rights (ECHR) and the right to privacy. The Commission echoes the concerns of the Information Commissioner in their detailed submission on this issue about “the scale of privacy intrusion, with the
potential to affect large numbers of people, in many cases without their knowledge, as they go about their daily lives”. Such an intrusion engages Article 8 ECHR and, the use of facial recognition in this manner can only be justified if it is proportionate to the state’s aim. There is presently no independent adjudicator of that proportionality exercise and this is of concern.

3. The purpose of using facial recognition technology. For example, Police Scotland’s practice of sharing images with UK police forces through the use of the Police National Database (PND), which has a ‘facial search’ facility: The submission of the Police Federation details the prospective uses of official recognition technology including facial mapping and, going beyond this, to include live facial recognition. As narrated above, the Commission is concerned about the lack of evidence of effectiveness, and therefore proportionality, surrounding facial recognition technology. We share the concerns detailed by Dr. Angela Daly in her submission which discusses evidence of the misidentification of innocent people and the disproportionate effect of inaccurate facial recognition upon black and minority ethnic people. The Commission is further concerned about the population of the Police databases having been constructed with few safeguards to protect people’s rights. Use of facial recognition on this basis prejudices outcomes. We refer to the IAG recommendation (6) (There should be a presumption of deletion of biometric data after the expiry of prescribed minimum retention periods) which was conceived in the knowledge that databases that retained biometric information indefinitely were likely to breach the right to privacy.

4. 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): The submission of the Information Commissioner has comprehensively analysed the data protection implications of the use of facial recognition technology. The Commission would be concerned if Police Scotland were to harness the use of facial recognition technology via a third party in the private sector who is not regulated. Such measures should be transparent and accessible. The Commission considers that state accountability and responsibility must be maintained for the protection and realisation of human rights.

5. The legal and regulatory basis that Police Scotland rely upon to use facial recognition technology: We welcome Police Scotland’s caution in introducing this technology in order to allow the Committee to take evidence on the issue. We look forward to having sight of both the Data Protection Impact Assessments and the Equality Impact Assessments that good practice dictates would be conducted prior to any use of this technology. Previous submissions by the Commission have established deficits within the legal framework for the use of this type of technology. The outcome of litigation in Wales\(^1\) supports the view that a statutory code should be considered. This is in line with the Government’s intention to create the post of Scottish Biometrics Commissioner with oversight over a Code of Practice governing the use of this technology.

---

\(^1\) R (Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin)
The Committee should be aware that there are a variety of facial recognition technologies including the facial matching that Police Scotland currently engage and live facial recognition which has been trailed and used in England and Wales. Wider public consultation should be undertaken to evaluate the public’s understanding of these technologies and their rights in relation to the same. Following this, a legal framework should be put in place that protects the public in a clear and accessible format. Evidence from stakeholders and independent experts should be sought to ensure that the technical capabilities are appropriately addressed in the law. There should be no use of facial recognition technology until these steps are undertaken. Failure to do so would risk damage to public confidence in the regulatory frameworks that protect their rights.

6. **The oversight, governance and transparency of Police Scotland’s use of facial recognition technology:** We refer to the Commission’s submission to the Scottish Biometrics Commissioner’s Bill. As facial recognition data is considered to be biometric in nature, all of the IAG recommendations are applicable to it. The submission of Privacy International itemises more detailed requirements as a pre-cursor to consideration of the use of facial recognition (p10) which are consistent with a human rights based approach. The Committee will be aware that there are indications of public support for police use of facial recognition technology\(^2\). It is crucial to evaluate such statements in the context of a rigorous public information campaign. The Commission considers that the public are entitled to transparent, accessible information of a high standard in order to understand the nature of the technology and how it could impact upon their rights. The submission of Glasgow City Council notes that erroneous information about their use of facial recognition is already in the public domain and seeks to correct this with detailed information. The Ada Lovelace Institute recommends that “For each distinct application of the technology there should be an appropriate form of public engagement, trials and an evidence base”. Their detailed model of public engagement is an example of the necessary evaluation that would be necessary to guard against breaches of human rights.

The Commission has previously given evidence to this Committee in respect of the Police and Fire Reform (Scotland) Act 2012 (the “Act”). The Commission in that instance recommended that

**A commitment to upholding human rights, as protected by the Human Rights Act 1998 (“HRA”), should be explicitly included in the policing principles of the Scottish Police Service provided for in section 32 of the Act.**

The Commission considers that this issue underlines the importance of this recommendation. Commitment to compliance with human rights standards is a necessary safeguard to ensure that the state allocates appropriate resources and ensures the responsibility of Police Scotland to take necessary measures in

\(^2\) Submission of Ada Lovelace Institute referred to by Police Federation of Scotland
compliance with the law. The Commission welcomes the intervention of the Justice Committee in addressing this issue and would welcome the opportunity to present evidence before the Committee.

Judith Robertson
Chair, Scottish Human Rights Commission
6 November 2019