Published 11 February 2020
SP Paper 678
1st Report, 2020 (Session 5)

The Scottish Parliament
Pàrlamaid na h-Alba

Justice Sub-Committee on Policing
Fo-chomataidh a' Cheartais air Obair a' Phoilis

Facial recognition: how policing in Scotland makes use of this technology

Published in Scotland by the Scottish Parliamentary Corporate Body.

All documents are available on the Scottish Parliament website at:
http://www.parliament.scot/abouttheparliament/91279.aspx

For information on the Scottish Parliament contact Public Information on:
Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

Contents

Justice Sub-Committee on Policing

To consider and report on the operation of the Police and Fire Reform (Scotland) Act 2012 as it relates to policing.

http://www.parliament.scot/parliamentarybusiness/CurrentCommittees/101581.aspx


justicecommittee@parliament.scot


0131 348 5220

Committee Membership

Convener
John Finnie
Scottish Green Party

Deputy Convener
Margaret Mitchell
Scottish Conservative and Unionist Party

Jenny Gilruth
Scottish National Party

James Kelly
Scottish Labour

Fulton MacGregor
Scottish National Party

Rona Mackay
Scottish National Party

Liam McArthur
Scottish Liberal Democrats

Executive Summary

The introduction of live facial recognition to policing in the UK is a relatively new phenomenon.

Police Scotland has an ambition, outlined in its 10-year strategy, to introduce its use by 2026. Its assessment of the likely equalities and human rights impact as "likely to be positive in nature" is in stark contrast to the evidence received by the Justice Sub-Committee on Policing.

The live facial recognition software which is currently available to the police service is known to discriminate against females, and those from black, Asian and ethnic minority communities.

For this reason, the Sub-Committee believes that there would be no justifiable basis for Police Scotland to invest in this technology.

We therefore welcome confirmation from Police Scotland that they have no intention to introduce it at this time.

Prior to any decision to introduce live facial recognition technology to policing in Scotland, it is essential that a robust and transparent assessment of its necessity and accuracy is undertaken, and that the potential impacts on people and communities are understood.

The use of live facial recognition technology would be a radical departure from Police Scotland's fundamental principle of policing by consent.

Police Scotland need to demonstrate that its use of this technology is provided for in legislation and meets human rights and data protection requirements.

This short inquiry has highlighted the pressing need for a much wider debate on the use of live facial recognition technology by the police service, as well as more widely across the public sector, and by private companies. Politicians could play a key role in determining whether there is public consent for the use of this technology.

The Sub-Committee hopes that this inquiry has gone some way to begin that debate, and that the Scottish Government will take up the challenge.

Police Scotland currently use retrospective facial recognition technology. Its procedures and practices would benefit from a review by the Scottish Police Authority and any incoming Scottish Biometrics Commissioner.

In particular, consideration of the risks and legal implications of Police Scotland accessing and using any images held illegally on the UK Police National Database of people who have not been convicted of any crime.

The same concerns arise from Police Scotland's ability to access and use images of people who have not been convicted of any crime, but which are retained on the legacy IT systems they inherited from the former Scottish police forces.

The Sub-Committee believes that the police must have all necessary tools at their disposal to combat crime and keep communities safe.

New technologies have the potential to assist Police Scotland in detecting and solving crimes. However, each new technology must be assessed on its merits, with an honest and transparent discussion of both the benefits and the risks.

The Sub-Committee warmly welcomes Police Scotland's intention to introduce the use of ethics panels to consult with relevant stakeholders to identify and mitigate risks, and to inform its decisions on whether to introduce new technologies.

Introduction

1. The Justice Sub-Committee on Policing undertook an inquiry, from October 2019 to February 2020, into how policing in Scotland makes use of facial recognition technology.

2. The inquiry remit was to consider whether the use of facial recognition technology by the police service in Scotland is lawful, ethical, necessary, proportionate and transparent.

3. The inquiry included consideration of the recent trials of the use of live facial recognition technology undertaken by police forces in England and Wales.

4. The Sub-Committee issued a call for evidence on 4 October and received a number of written submissions from organisations, academics and individuals. It held three oral evidence sessions [1] , concluding on 16 January 2020.

5. The Sub-Committee would like to thank all those who provided written and oral evidence, which has been invaluable in informing its scrutiny of this issue.

Background

Developments in policing in Scotland

6. In January 2016, Her Majesty's Inspectorate of Constabulary in Scotland (HMICS) published a report titled *Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland*. [1] It was published after the matter was raised with the First Minister and the Cabinet Secretary for Justice in May 2015 at the Scottish Parliament, leading to Ministers discussing the matter with HMICS. The review's recommendations included that the "Scottish Government should work with Police Scotland and the Scottish Police Authority to consider legislative provision in relation to the retention and use of photographic images by the police".

7. In June 2017, Police Scotland published Policing 2026, its 10-year strategy for policing. The strategy was jointly and collaboratively developed with the Scottish Police Authority (SPA), who have responsibility to maintain the police service and to hold the Chief Constable to account.

8. The strategy outlines the vision for Police Scotland over the next 10 years. That includes the introduction of a number of new technologies, such as smart devices which can access and download images from a local authority app, embedded body-worn video cameras, mobile devices, and the use of facial recognition technology.

9. The Sub-Committee recently undertook an inquiry into Police Scotland's intention to deploy the use of digital device triage systems[i] (known colloquially as cyber kiosks), from September 2018 to frontline police officers to search mobile devices throughout Scotland. The Sub-Committee raised a number of issues within its report, including ethical, privacy, legal and data protection concerns. As a result, Police Scotland postponed introduction until January 2020 to take time to resolve those concerns to their satisfaction, albeit other key stakeholders continue to have concerns about the legal basis for deployment.

10. In September 2019, HMICS published a report [2] on its Thematic Inspection of the Scottish Police Authority. The report included the Sub-Committee's scrutiny of the proposed introduction of cyber kiosks as a case study, and identified a number of key learning points for the SPA and Police Scotland.

11. The Inspectorate found that impact assessments had not been carried out prior to Police Scotland and the SPA purchasing the equipment and planning to deploy it, stating that:

> "there was insufficient consideration given to human rights, equality and community impact assessment of wider access to digital triage devices by Police Scotland". [2]

---

i Digital device triage systems, known colloquially as cyber kiosks, would enable frontline police officers to search mobile devices of suspects, witnesses and victims of crimes.

12. The Inspectorate also found that the oversight of the proposal to introduce this new technology was inadequate, saying that:

> "The SPA failed to consider the full implications of the 3 year implementation plan and had inadequate change governance and proactive risk identification arrangements in place". [2]

13. HMICS had previously recommended, in 2014, that Police Scotland should adopt a comprehensive stakeholder management process and apply community impact assessments as a matter of course. This recommendation was not implemented and was reiterated in the 2019 inspection report.

14. HMICS also recommended that the SPA and Police Scotland develop a forward planning system of proactive risk awareness and post-implementation scrutiny for policing policy changes which are likely to have an impact on public confidence. [2]

15. During the Sub-Committee's inquiry into the use of facial recognition technology by the police service, the Justice Committee of the Scottish Parliament was considering a Bill to introduce a Scottish Biometrics Commissioner and establish a code of practice for the acquisition, retention, use and disposal of biometric data for criminal justice and police purposes. The Sub-Committee considered the recommendations in the Justice Committee's Stage 1 report, which related to facial recognition technology, and the Scottish Government's response to those recommendations.

How does facial recognition technology work?

16. Biometric technologies for facial recognition require an image to analyse. This could be a still photograph like those taken by systems at airports, or a frame from a video of a person in motion. Some systems also use techniques such as thermal imaging sensors to obtain additional information. As a result, the 'image' to be analysed might actually be a set of images created by different types of sensors.

17. The system searches for a face or faces in the image. It looks for characteristics that indicate the presence of a face, such as eyes, ears, nose, mouth, and cheekbones. Once it identifies enough of these, the system has 'found' a face.

18. The system also measures various characteristics of the face. Some characteristics that might be used are the distance between the eyes, the depth of eye sockets, the shape of cheekbones, and the distance from the forehead to the chin. Newer systems generally consider many more characteristics than this, such as skin colour and texture. They can also make adjustments, for example for variable lighting, or to identify a face that is not looking directly into the camera. The resulting data is stored as a representation of a face.

19. The representation of that face is then compared to a database of known faces, which are sometimes referred to as a "watchlist". The system identifies the best match amongst the faces in the database and determines whether the match is close enough to be considered a 'hit'. Police officers, or the operators, would then verify the matches to ensure that they are accurate before proceeding to engage with possible suspects.

20. The use of facial recognition technology can be live, which means that it is in real-time, or retrospective, which would be post-event, such as the scanning of pre-recorded video footage.

21. The UK Biometrics and Forensics Ethics Group in England and Wales define [3] live facial recognition technology as: "the automated one-to-many 'matching' of real-time video images of individuals with a curated "watchlist" of facial images".

22. Retrospective facial recognition is the use of facial recognition technology to search through recorded surveillance camera or other video footage, matching people's faces captured in that footage against a database of images.

23. The Sub-Committee considered Police Scotland's plans to introduce the use of live facial recognition technology, its current use of retrospective facial recognition technology, and the potential role that a Scottish Biometrics Commissioner might have, should the establishment of this post be agreed by the Scottish Parliament.

Live facial recognition technology

24. The Sub-Committee considered Police Scotland's proposal to introduce the use of live facial recognition technology.

25. In their written submission, Police Scotland state that they are not currently using or trialling live facial recognition technology in a live setting or public space. However, they also confirm that it is their intention to "explore the use of all available investigative techniques, including the use of facial recognition technology" [2] .

26. Police Scotland indicate their intention to await until the enactment of the provisions of the Scottish Biometrics Commissioner Bill, before introducing the use of live facial recognition software. [3]

27. In their submission, the Scottish Police Federation, highlight the ways in which the use of facial recognition applications could assist policing and public safety. This includes searching for missing children, vulnerable adults or wanted persons, and comparing suspect images against a gallery of known criminals to assist in identifying perpetrators more quickly, than could be done manually. They conclude that the technology offers an opportunity for Police Scotland to work more efficiently and effectively, saying that:

> "Some work will be needed to set out rules and codes within which the Service can operate but this must not be burdensome or overly bureaucratic". [4]

Policing 2026

28. The Policing 2026 [4] 10-year strategy includes two scenarios where police officers use facial recognition technology.

29. In the scenario of the 'day in the life of a police officer in 2026', the strategy refers to the officer uploading footage from a body-worn video camera and accessing and downloading images from a local authority CCTV app on their mobile device. The scenario is described as follows:

> "I access the local Council CCTV app on my device and observe the assault has been captured. I download the footage I need. The suspect has been recognised by facial recognition software and I send out a live time briefing alert across the division, the Police National Computer system is updated automatically. The suspect is quickly arrested by another local team". [4]

30. In their written submission, Liberty highlight the lack of detail in Policing 2026, saying the facial recognition technology references: "are not detailed, and simply indicate a desire to use the technology to identify suspects". [5]

31. In their joint submission, the Open Rights Group [ORG] and Big Brother Watch [BBW] also highlight a lack of clarity, as Policing 2026 does not make clear whether facial recognition technology is to be applied to CCTV still images or video, stating that:

> "It's important to be clear about exactly what form of facial recognition technology is being used or proposed, as each distinct use engages people's legal rights in different ways or engages different rights". [6]

32. In the second scenario in Policing 2026, there are a number of thefts by multiple suspects at a shopping centre. One of the centre's security guards logs on to the police self-service portal using his smart device, to report the thefts. He then uploads the evidence, such as CCTV footage, editing the file online to focus on the crime's time frame. The strategy states that Police Scotland will access this information in the following way:

> "A crime and investigation log is automatically populated. Artificial intelligence (AI) scans the footage, identifying a main suspect via facial recognition however images of the accomplices are too blurry. An intelligence file is automatically populated with a suspect profile including associates attached to the log. The AI begins to build an evidence case … The information report highlights the shopping centre as an emerging 'hot spot' and identifies the suspect". [4]

33. In their written evidence, the Ada Lovelace Institute raise similar concerns about a lack of detail within this scenario, saying it provides "no further evidence or clarification regarding how the expectation of benefit and safeguards are addressed". The Ada Lovelace Institute recommend that:

> "There is a need to pause and take stock of how facial recognition will be applied, for greater clarity on scenarios and preparation for their adoption into practice". [7]

Equality and human rights impact assessment

34. The SPA and Police Scotland carried out an equality and human rights impact assessment (EqHRIA) of the Policing 2026 strategy and published a summary of results, [5] in March 2018.

35. The summary indicated that there would be "no direct or indirect adverse or disproportionate impact on protected groups in the wider community or in respect of partnerships" from the implementation of Policing 2026. The summary concludes that:

> "Any impact is likely to be positive in nature, as the proposed strategy will identify potential for inequality and disadvantage at an early stage through ongoing community engagement and the focus on threat, risk and harm to people, places and communities". [5]

36. In their written submission, Liberty describe this conclusion as "a matter of grave concern", saying that:

> "... the Equality and Human Rights Impact Assessment (EqHRIA) carried out in relation to the strategy concluded that a *"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". [8]

37. Liberty state that the lack of analysis of the impact of introducing technology which is discriminatory, falls short of the requirements for Police Scotland in section 149(1) of the Equality Act 2010. Section 149(1) (a) of the Act places a duty on the public sector to have regard to the need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by, or under, the 2010 Act. [9]

38. The Sub-Committee heard that there is much research and evidence which indicates that live facial recognition software has an in-built gender and racial bias, and is therefore discriminatory. This issue is covered in more detail later in the report.

39. Despite the commitment to carry out on-going community engagement as Policing 2026 is implemented, the Sub-Committee heard during its inquiry into the proposed introduction of the use of cyber kiosks that this engagement was not deemed necessary.

40. During the inquiry Police Scotland confirmed that no human rights, equalities, community impact, data protection or security assessments were carried out prior to undertaking operational trials of the equipment. The former interim Chief Officer of the SPA also stated that he did not believe that a community impact assessment was required for the introduction of cyber kiosks, as it was not a change to operational policing. [10]

Legal basis for the use of live facial recognition technology

41. A key issue raised in evidence is whether legislation has kept pace with technological developments, and whether it is sufficiently clear to enable people to understand when their biometric data may be processed by live facial recognition technology.

42. The Sub-Committee considered the legal basis upon which police forces in Scotland, and in England and Wales, rely to collect, use and retain biometric data.

England and Wales

43. Police forces in both England and Wales have recently trialled the use of live facial recognition technology. The Sub-Committee heard that they relied upon a mixture of common law powers, data protection and human rights legislation, and the Police and Criminal Evidence Act 1984.

44. Dr Joe Purshouse, from the University of East Anglia, explained that the common law powers being relied upon are general in nature and were made prior to facial recognition technology being developed. Dr Purshouse added that:

> Whether that provides a sufficient legal basis or power to use the technology might be questioned.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 5[6]

45. Dr Christopher Lawless, from Durham University, expressed a concern about the "fairly unregulated approach to the collection of images" by police forces in England and Wales. He indicated that this is because the Protection of Freedoms Act 2012 ('the 2012 Act') only covers certain forms of biometrics, such as DNA, fingerprints and footprints. Dr Lawless suggested that the 2012 Act could be extended to include facial images, saying:

> That leads me to wonder whether the Protection of Freedoms Act 2012 could be made clearer on facial data or could be extended to cover facial images explicitly.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Christopher Lawless (Durham University), contrib. 7[7]

Legal challenges

46. South Wales Police ('SWP') and the Metropolitan Police Service ('MPS') have both faced legal challenges to their trials of the use of live facial recognition technology.

47. In the 2019 case of *R (on the application of Bridges) v Chief Constable of South Wales Police*, (SWP) [8] the adequacy of the current legal framework was considered in relation to two trials of the use of live facial recognition technology, called AFR Locate, undertaken by SWP.

48. The judgement considered common law powers and the legal framework. It found the police's common law powers to be "amply sufficient" in relation to the use of AFR Locate, and that "there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used". It also found that the use of AFR Locate was "consistent with the requirements of the Human Rights Act, and the data protection legislation". [8]

49. The judgement stated that "we do not consider that the legal framework is at present out of kilter; yet this will inevitably have to be a matter that is subject to periodic review in the future". [8]

50. The Sub-Committee heard that the judgement is currently subject to appeal and the case against the Metropolitan Police Service is currently stayed.[ii]

51. Following the judgement from the High Court in Cardiff, the UK Information Commissioner ('ICO'), Elizabeth Denham, issued an opinion[iii] on the use of live

---

ii [1] A stay of proceedings is a ruling by the court in civil and criminal procedure, halting further legal process in a trial or other legal proceeding. The court can subsequently lift the stay and resume proceedings based on events taking place after the stay is ordered. However, a stay can be used as a device to postpone proceedings indefinitely.

facial recognition technology by law enforcement in public places. The Opinion [9] stated that:

> "While the legislative framework underpinning the use of LFR is evolving, the Commissioner does not consider that the decision of the High Court should be seen as a blanket authorisation to use LFR in all circumstances …Taking full account of the High Court's judgment, the Commissioner believes that there are areas of processing personal data where the police should seek to raise the standards beyond those set out in the judgment when deploying LFR in public spaces in order to ensure public confidence in this technology".

52. The UK Information Commissioner's Opinion is considered in more detail in the section in this report on compliance with data protection legislation.

53. Dr Ken Macdonald, Head of ICO Regions, told the Sub-Committee that the use of facial recognition is a high priority for the UK Commissioner. The Commissioner's view is that its use should be considered on a case-by-case basis, and that the police service should explain the reason why the use of the technology is necessary, in each circumstance. Referring to the judgement, Mr Macdonald said:

> In that case, the court found that use of the technology had been lawful, bearing in mind all the other restrictions that are in place, including data protection legislation. Our view is that that judgment was on a specific case and cannot be applied as a general framework.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Dr Macdonald, contrib. 19[10]

54. In their written evidence, the Law Society of Scotland indicate that the judgement in the case of South Wales Police will have implications for Scotland. In particular, with regards to meeting data protection and human rights requirements and the provisions of the Equality Act 2010. The Law Society state that:

> "We would stress that though the decision in that case may have found in favour of the police, that seems far from the end of the discussions. There are calls for a facial recognition technology code of conduct to be produced for England and Wales while Liberty, who brought the case are campaigning for a ban". [11]

55. In evidence to the Sub-Committee Dr Purshouse and Dr Lawless both highlighted the specific context of the case. Dr Lawless questioned what might have happened had the case involved adverse consequences for an individual as a result of a false positive identification. [12]

56. Dr Purshouse outlined the inconsistent practices adopted by different police services, due to a lack of regulation. This means that some have used the technology for serious crimes only, whilst others have applied it more broadly. Examples include sourcing images from multiple sources or solely from custody images, and pursuing cases of non-criminal infractions and anti-social behaviour, or focussing on strict criminality. [13]

---

iii [2] Schedule 13 of the Data Protection Act 2018 provides the Commissioner with the power to issue … opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

57. Matthew Rice from the Open Rights Group described the South Wales Police judgement as narrowly based, and not a green light for facial recognition technology to be deployed on a large scale. Mr Rice added that:

> the scope of intrusion that facial recognition would involve would make a challenge likely in Scotland.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 21[11]

Scotland

58. The Sub-Committee considered the legislative framework being relied upon for the use of live facial recognition technology in Scotland.

59. In their written submission, Police Scotland indicate that they will explore and invest in new technologies, including facial recognition, "subject to regulatory parameters". [14]

60. The Scottish Government established an independent advisory group (IAG) on the Use of Biometric Data in Scotland in June 2017. Its remit included advising Scottish Ministers on a policy and legislative framework for the capture, storage, retention, use and disposal of biometric data. This included facial images and other forms of emerging biometric data. It also included reviewing the retention of custody images[iv] by Police Scotland.

61. The IAG report [12] highlighted the Criminal Procedure (Scotland) Act 1995 ('the 1995 Act') as the primary Scottish legislation, which allows the retention of fingerprints and other biometric samples from a person arrested by the police. However, the 1995 Act does not refer to facial images.

62. The IAG concluded in its report that a legislative framework for the use of biometrics "was not only desirable but necessary, in order to satisfy the obvious requirement of lawfulness for such activity". [12]

63. In their written evidence, HMICS highlight the risks of legal challenge to the use of live facial recognition technology in Scotland, stating that:

> "In the absence of any specific legal framework or Codes of Practice in Scotland, it is highly likely that any future deployment of AFR/LFR in Scotland would be contested and that the lawfulness of a specific application would need to be determined in the Scottish Courts. In this regard, it would be essential not only that the actual activity by the police itself was lawful, but also that the specific technology solution in question was reliable and non-discriminatory". [15]

64. In their submission, the Law Society of Scotland recognise that developments in biometric data are fast moving and indicate that there would be considerable benefit in producing a regulatory framework for the use of facial recognition technology, stating that:

---

iv A custody image is a photograph of an individual taken when processed at a police station of a suspect or accused person.

> "The legal and regulatory basis for the use of facial recognition in Scotland on which Police Scotland will rely needs to be developed in the light of experience from other jurisdictions". [13]

65. In their written evidence, the Crown Office and Procurator Fiscal Service (COPFS), indicate that should an evidential product from the use of facial recognition technology lack legal authority, it may still be admissible as evidence, saying that:

> "Where the evidential product is outside the terms of, or lacks, lawful authority then the evidence will not necessarily be inadmissible. In that instance, the fairness of the approach taken by the Police will be considered by prosecutors and, if prosecuted, by the courts to assess whether the evidence will be admissible. Each case will be determined on its facts and circumstances". [16]

66. In response to a question on whether the "fairness of approach" is a robust enough test, Dr Purshouse described fairness as a subjective term. He cautioned that there is a balance to be struck to ensure prosecutions of serious crimes are not jeopardised by a technical oversight. [17]

67. The Ada Lovelace Institute carried out research, via an on-line survey, to understand public attitudes to the use of facial recognition technology by both the public and private sectors. They found that nearly half of those who responded expressed the belief that they should be able to opt out of, or consent to, facial recognition technology being used. The Ada Lovelace Institute concluded that:

> "In practice, this and other safeguards are often missing. There is a need to review and clarify the legal framework for facial recognition and ensure it keeps apace with public expectations". [13]

68. In her published Opinion, the UK Information Commissioner recommends that a statutory code of practice be considered by the UK Government "at the earliest opportunity", to address concerns about necessity, proportionality, privacy intrusion, and public confidence. [9]

69. However, in her written evidence, Dr Angela Daly from the University of Strathclyde Law School, questions whether a statutory code would be sufficient to address concerns about mass-monitoring where there is no social licence to do so. Dr Daly highlights the decisions of other cities and regions to prohibit the use of facial recognition technology. [18]

70. Dr Lawless told the Sub-Committee that a Scottish Biometrics Commissioner, a code of practice, and clear guidelines should be in place before live facial recognition technology is used. He indicated that developing a code of practice and guidelines should be a priority for the Biometrics Commissioner, as it would provide: "an understanding on the part of the police of the rules within which they can manoeuvre". [19]

71. Dr Purshouse said that it is the role of parliamentarians, and others, to provide the police service with clear guidance and legal limits for the technologies that they wish to introduce to prevent and detect crime. Dr Purshouse told the Sub-Committee that:

> It is the sub-committee's job and our job to set those standards. We must lead the way in thinking ahead to what technologies might be coming down the pipeline or are starting to emerge and take a proactive role in deciding what the appropriate democratic limits are and what the use of that technology in a human rights-compliant way might look like. There is a pattern here: the police use a technology and try to guess what the limits are, and then there is the back and forth of legal challenges, with regulation seeming to play catch-up. That is why I welcome you doing this work.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 84[14]

72. Dr Anna Bobak from the University of Stirling agreed with this view. Dr Bobak welcomed the current debate, adding that in her opinion,

> a legal framework and clear guidance are paramount ahead of the rolling out of any live facial recognition software.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Bobak, contrib. 85[15]

73. Temporary Assistant Chief Constable ('T/ACC') Duncan Sloan of Police Scotland reiterated the force's position that they "do not intend, at this point in time, to trial any live facial recognition technology". T/ACC Sloan told the Sub-Committee that, as trialling and testing of the technology is ongoing elsewhere in the UK, Police Scotland would welcome a legal framework, saying:

> we would welcome a legal framework in order to maintain legitimacy for Police Scotland and to have the consent of the people.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 44[16]

74. T/ACC Sloan added that, before embarking on a course of action to use live facial recognition technology, Police Scotland would also welcome a wider public debate with interested parties, to help understand the nature of the technology and how it would be used. [20]

75. Lynn Brown, interim chief executive of the Scottish Police Authority, described a clear legal basis for the use live facial recognition technology as "essential" and a proposed code of practice as "welcome". Ms Brown explained that the SPA's role would be to make sure that Police Scotland was abiding by that code of practice, adding that:

> We have an opportunity to give the public the confidence that we are approaching it in an appropriate manner.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Lynn Brown (Scottish Police Authority), contrib. 48[17]

Compliance with human rights legislation

76. The Sub-Committee considered whether the use of live facial recognition technology by Police Scotland would meet the legal requirements of the European Convention on Human Rights (ECHR).[v]

Accuracy and effectiveness

77. The Sub-Committee heard that there are significant concerns about the level of inaccuracy and ineffectiveness of live facial recognition software. The Sub-Committee considered whether current technology is fit for purpose.

Gender and racial bias

78. A key concern raised in evidence was the gender and racial bias that is in-built within live facial recognition software.

79. The UK Biometrics and Forensics Ethics Group published an interim report in February 2019 on *Ethical issues arising from the police use of live facial recognition technology.* [3]

80. The Group highlighted concerns about racial and gender bias in a number of areas, such as training datasets employed to develop the software algorithms for facial recognition, and bias by human operators in their response to the outputs of the LFR technology. The Group found that:

> "If certain types of faces (for example, Black, Asian and Ethnic Minority faces or female faces) are under-represented in LFR training datasets, then this bias will feed forward into the use of the technology by human operators. There have been high-profile scientific concerns that there is intrinsic potential racial and gender bias within LFR systems". [3]

81. Biometric technologies for facial recognition require machine-learning algorithms that have been trained on a dataset of labelled images. The system can only 'recognise' faces within the parameters of the data that it has been trained on and previously exposed to. The Sub-Committee heard that one of the issues with the technology is that the police service would not have the authority to change those algorithms, and eliminate any potential bias or discrimination.

82. Dr Bobak explained that ethnic and gender bias is a result of the training set images on which the algorithms are based. Dr Bobak explained that, for example, if the data set are predominantly Caucasian males, then the algorithm will be biased towards higher accuracy for those types of faces.

83. Dr Bobak stated that, as the police have no control over the algorithms used and the level of accuracy "the police need to be quite wary about the claims that some of the technology providers make". [21]

84. Matthew Rice highlighted to the Sub-Committee that the police service are relying on the ethics of the commercial providers when investing in this technology, stating that:

> We are in essence relying on another organisation's ethics and the decisions that it has taken in the development of its technology to determine whether it is ethical and accurate or encoded with the biases that we have seen so far.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 46[18]

---

v European Convention on Human Rights.

85. Griff Ferris of Big Brother Watch described the level of inaccuracy of the technology as a serious concern. He referred to information published in 2017 by the Metropolitan Police Service that the inaccuracy rate of the technology they used was 98%, and the inaccuracy rate from the technology that South Wales Police had used was 91%. Mr Ferris stated that "… this is an incredibly inaccurate technology that misidentifies people at much higher rates than it identifies them". [22]

86. Mr Ferris described the discrimination and racial and gender bias within the technology as "extremely serious". He added that: "Notwithstanding that, the fact that the technology has that discrimination bias should be enough to disqualify its use on that ground alone". [23]

87. In her written evidence, Dr Angela Daly highlights the risks of the police service misidentifying people, saying that:

> "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". [24]

88. Matthew Rice explained to the Sub-Committee that the implications of the inaccuracy of the technology are serious, as a person could be detained solely on the basis of the facial recognition technology analysing their facial features, and does not require any other corroborating evidence. [25]

89. In their written submission, the Law Society of Scotland highlight the need to test and challenge in-built biases. However, they question whether that is possible as the algorithms used are likely to be considered as commercially sensitive intellectual property, meaning that in reality only the outcomes of the technology can be analysed. [26]

90. Dr Macdonald told the Sub-Committee that the UK Information Commissioner is of the view that it is important to review the effectiveness of the impact of the technology, given the high number of mismatches of females and those from ethnic groups. [27]

91. In the UK Information Commissioner's published Opinion, Ms Denham describes effectiveness as a "key consideration when it comes to strict necessity and proportionality". The Opinion states:

> "The Commissioner notes that, without clear evidence of effectiveness based on a thorough and transparent evaluation process, it is difficult to see how the strict necessity threshold could be reached or how the intrusion into individuals' rights and freedoms could be considered proportionate. [9]

92. Tatora Mukushi from the Scottish Human Rights Commission (SHRC) questioned whether the police service investing in technology with such a low accuracy level provided best value for money. Mr Mukushi told the Sub-Committee that: "If Police Scotland were to invest in technology that had this failure rate, there would rightly be a public outcry, because it is hardly effective or efficient". [28]

93. Griff Ferris told the Sub-Committee that Police Scotland risked a human rights legal challenge, saying that:

> As has been mentioned, it is a very serious threat to the right to privacy and the right to freedom of expression and association, and there are serious concerns about its discriminatory use, notwithstanding its general complete ineffectiveness as a technology.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Griff Ferris, contrib. 20[19]

94. T/ACC Sloan confirmed that live facial recognition technology would need to improve before it was introduced by Police Scotland, with serious consideration given to its reliability, saying that:

> Facial recognition technology has a long way to go before we would get to the stage of using it—if we ever would. As with other techniques and tactics that are used by Police Scotland, that would be strictly intelligence led and targeted. We are not about to embark on use, but if we were to do so, it would be along the lines of necessity and proportionality.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 46[20]

95. T/ACC Sloan added that the use of technology by Police Scotland "must be balanced against the need to respect human rights and privacy", and that there is a need for a "wider debate on policy and what the public expects and would consent to", so that what the police service do is legitimate.

96. T/ACC Sloan explained that Police Scotland is in the process of setting up a framework for data ethics, and their intention is to involve civil liberties groups and academics in the process, to enable the police service to take a more holistic approach. [29]

97. Tom Nelson, Director of Forensic Services at the SPA, told the Sub-Committee that the Scottish Police Authority must ensure that it tests and understands the limitations of any new technology, and how intrusive or otherwise it might be, before any decision is made to roll it out. Mr Nelson confirmed that an assessment of facial recognition technology would include consideration of its accuracy and the disproportionate results in relation to race and gender, saying that:

> We must ensure that the whole system has been tested and validated before it is taken to the next stage, which would be to put together a business case.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Tom Nelson (Scottish Police Authority), contrib. 68[21]

98. Lynn Brown, agreed, adding that the financial appraisal process should include aspects such as the effects of the technology on the rights of individuals, and whether it met all the public interest requirements. [30]

Quality assurance

99. The Sub-Committee heard that quality assurance processes should be created to test the accuracy and effectiveness of the technology.

100. Dr Bobak recommended that the police service ask a computer scientist to check the claims of the software providers, before investing in the technology. [31]

101. Dr Lawless suggested that a Scottish Biometrics Commissioner could verify the claims of reliability and accuracy of the commercial providers, and agree basics standards. He also referred to calls to publish data on the performance of facial recognition technology, and that this should apply to other forms of biometric data. [32]

102. Tom Nelson indicated that he hoped that a code of practice, introduced by any Scottish Biometrics Commissioner would include a process to validate the roll-out of new technology. However, Mr Nelson added that the SPA Board would have to demonstrate to the Commissioner that it had gone through a reliable process. [33]

103. Lynn Brown explained that when undertaking a public procurement exercise, the SPA can bring in expert advice to assist in making decisions on best value. Ms Brown indicated that this could be necessary for the procurement of live facial recognition technology. [34]

Necessity and proportionality

104. Questions were raised in evidence about whether it was necessary for the police service to introduce the use of live facial recognition technology, whether mass surveillance of the public by the police service was proportionate, and whether the public have trust in its use.

105. In their written evidence, the Law Society of Scotland state that obtaining public confidence in the use of facial recognition technology is essential. They indicate that this means striking the right balance between invasion and crime detection, saying that:

> "That means the balance has to be maintained between the inevitable invasion of individual privacy that arises with the use of facial recognition, the potential clash with Article 8 of the European Convention on Human Rights and the public and State benefit that derives from the use of such technologies in furtherance of the detection of crime".[vi]

106. Dr Purshouse told the Sub-Committee that it is for those impacting on human rights to justify the necessity and proportionality of the use of live facial recognition technology, and to explain why the same benefits could not be achieved through less intrusive means. Dr Purshouse cautioned that failure to do so could impact on public confidence in the police service, saying that:

---

vi Law Society of Scotland, written submission, page 3.

> Ultimately, it could damage the legitimacy of the police if it is seen to be an intrusive technology that has been rolled out in ways that the public do not necessarily understand or trust.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 11[22]

107. In their joint written submission, the Open Rights Group and Big Brother Watch recommend that the use of facial recognition technology by Police Scotland, or any public body, should be transparent and subject to public consultation, stating that:

> "We call on the Committee to obtain clear and comprehensive information from Police Scotland, and any other public body which intends or proposes to use a type of facial recognition technology, about exactly which type of technology they propose to use and its capabilities. Any such proposals should be subject to public consultation".[vii]

108. Dr Bobak told the Sub-Committee that there remain unanswered questions about how the technology could be used in a proportionate way in open spaces. These include circumstances where searches are not focussed, and also when facial recognition data is collected from children.[viii]

109. In his written evidence, Dr Garfield Benjamin from Solent University, raises a particular concern about the police service collecting and retaining data on children without their consent, saying that:

> "The UK Children's Commissioner released a report on children's privacy and the shocking amount of data that is collected and shared about children, often without their permission or even knowledge. The report highlights how more needs to be done to ensure that children's privacy is respected, and researchers have found that children want greater transparency over their data".[ix]

110. Griff Ferris told the Sub-Committee that the use of live facial recognition technology was not necessary or proportionate and was in breach of Article 8 of the ECHR, on the right to privacy. Mr Ferris explained that it had not been used solely to target serious criminals, but had been used at peaceful political protests and demonstrations, as well as on people who had not committed any crime. Mr Ferris explained that South Wales Police had scanned an estimated 500,000 people, and made 30 arrests. He added that, that level of intrusion without consent, meant that the technology could never be compatible with human rights, saying that:

> It is very much our view that, because of the indiscriminate nature of the technology—it scans everybody within view—it captures their image without their consent and potentially without their knowledge.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Griff Ferris, contrib. 28[23]

111. Matthew Rice highlighted to the Sub-Committee that in a situation where there is mass capture of facial images in public spaces, the public are not able to opt-out of

---

vii Joint Open Rights Group and Big Brother Watch written submission, page 1.
viii Justice Sub-Committee Official Report, 21 November, col 8
ix Dr Garfield Benjamin, Solent University, written submission, page 3.

having their biometric data taken. Mr Rice indicated that this impacts on their right to individual liberty. [x]

112. Dr Macdonald told the Sub-Committee that the UK Information Commissioner's Opinion included the need for the use of the technology to be proportionate. This would include a strong legal framework to ensure that the technology was only used when necessary, that its use should be narrow in focus to reduce those being scanned, that it should be used for a short period of time and not 24 hours a day, and that prior to its use a data impact assessment should be carried out to consider the impact on human rights.[xi]

113. Dr Macdonald added that the ICO would have concerns if facial recognition technology was used as a "fishing exercise", as that "would be entirely unacceptable and no doubt in breach of people's Article 6 rights" to a fair trial under the ECHR .[xii]

114. Dr Macdonald indicated that the implementation of a code of practice on the use of facial recognition technology, after a wide consultation, would help to address some of the concerns.[xiii]

115. Griff Ferris said that whilst he did not believe that the technology should ever be used, prior to any use there should be a legal basis, effective oversight, and a human rights analysis of its impact.[xiv]

116. Tatora Mukushi told the Sub-Committee that a Scottish Biometrics Commissioner, a strict code of practice, and enforcement powers, overseen by the Scottish Parliament would provide the police service with an accountability framework. However, Mr Mukushi added that:

> I have my reservations and, as the technology stands, there is unfortunately far too much evidence of its failings as opposed to evidence of its real usefulness.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Tatora Mukushi, contrib. 37[24]

117. Griff Ferris, Mathew Rice, Tatora Mukushi and Dr Ken Macdonald all agreed that community, privacy and equalities impact assessments should be carried out prior to the deployment of the technology in open spaces. Dr Macdonald also highlighted to the Sub-Committee the importance of engagement, and the need for a much wider debate on the use of live facial recognition technology.[xv]

---

x Justice Sub-Committee Official Report, 5 December, col 8
xi Justice Sub-Committee Official Report, 5 December, col 9
xii Justice Sub-Committee Official Report, 5 December, col 18
xiii Justice Sub-Committee Official Report, 5 December, col 9
xiv Justice Sub-Committee Official Report, 5 December, cols 9-10
xv Justice Sub-Committee Official Report, 5 December, cols 16-17

Compliance with data protection legislation

118. The Sub-Committee considered whether the use of live facial recognition technology by Police Scotland would meet the requirements of the Data Protection Act 2018 (the 2018 Act).[xvi]

119. Section 35 of the 2018 Act states that the first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair. In her issued Opinion, the UK Information Commissioner, Elizabeth Denham, said that:

> "The controller must identify a legal basis that provides a sufficiently clear, precise and foreseeable lawful justification to utilise LFR for the law enforcement purposes". [9]

Strict necessity

120. Section 35 (5) (a) provides that the processing of sensitive data is permitted if "the processing is strictly necessary for the law enforcement purpose".

121. The Sub-Committee considered whether the use of live facial recognition technology by Police Scotland would strike the right balance between the strict necessity of the processing of sensitive data and the rights of individuals.

122. The UK Information Commissioner describes the strict necessity requirement as "key" for the use of live facial recognition technology in public spaces. Ms Denham also recommends that law enforcement agencies should give more detailed consideration to the proportionality of the use of live facial recognition set against the intrusion that arises. [9]

123. The Commissioner also recommends that a detailed data protection impact assessment (DPIA) be completed prior to each deployment of live facial recognition technology, whether for a trial or other operational purpose. It should document both the risks posed and the safeguards necessary to mitigate them. [9]

124. Dr Macdonald explained to the Sub-Committee that there are two data protection issues for the police service to consider when deciding whether to use live facial recognition technology. These are whether there is consent and whether its use is strictly necessary. Dr Macdonald said that both are difficult to meet. He described meeting consent requirements for use in public spaces as "a totally impractical condition", and strict necessity as "a very high bar". Dr Macdonald added that:

> It would have to be clearly demonstrated why using facial recognition technology was appropriate when it was being deployed, and why other policing methods could not be employed to get the same result.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Dr Macdonald, contrib. 23[25]

125. In their submission, the COPFS state that it is for Police Scotland to satisfy themselves that data protection and human right requirements are met, saying that:

---

xvi Data Protection Act 2018.

> "The data protection, security and retention and human rights implications of the potential use of facial recognition technology are matters on which Police Scotland, as a public authority, must satisfy themselves. The involvement of COPFS relates to the admissibility in Court of any evidential product of facial recognition technology". [35]

Consent

126. Section 32 of the Police and Fire Reform (Scotland) Act 2012 ('the 2012 Act')[xvii] sets out the policing principles for Police Scotland. These are—

"(a) that the main purpose of policing is to improve the safety and well-being of persons, localities and communities in Scotland, and

(b) that the Police Service, working in collaboration with others where appropriate, should seek to achieve that main purpose by policing in a way which—

(i) is accessible to, and engaged with, local communities, and

(ii) promotes measures to prevent crime, harm and disorder".

127. The Sub-Committee considered whether there is public consent for the use of live facial recognition technology by the police service, and whether its introduction would meet the policing principles set out in the 2012 Act, and the stated ambition of Police Scotland to police by consent.

128. Police Scotland's 10-year strategy, Policing 2026, emphasises their core commitment to a rights-based approach to policing by maintaining public trust and consent, describing this as "key to our continued effectiveness, relevance and legitimacy". [4]

129. As live facial recognition technology has not been used by Police Scotland, very little research has been undertaken on public attitudes to its use in Scotland.

130. In July 2019, the Ada Lovelace Institute carried out research, via an on-line survey, to understand public attitudes to the use of facial recognition technology by both the public and private sectors. The research report included the following 6 key findings:

1. Most people do not know enough about facial recognition technology to have an informed opinion on its use.

2. The ability to consent to, or opt out of, facial recognition technology is an important safeguard.

3. People fear the normalisation of surveillance, but will accept facial recognition technology when there is a clear public benefit.

---

xvii Police and Fire Reform (Scotland) Act 2012.

4. There is no unconditional support for police to deploy facial recognition technology.

5. The public does not trust the private sector to use facial recognition technology ethically.

6. Companies and the government should act now. [13]

131. The research report also found that:

> "The public's support for the police's use of facial recognition technology is limited to specific circumstances. The public expects safeguards to be in place and to see a demonstrable impact on reducing crime. Nearly one third of the public are uncomfortable with police use of facial recognition technology, and those voices need to be reflected in debate on policy and practice". [13]

132. Tatora Mukushi described the introduction of new technologies to policing, as a change to the culture of policing by consent, which is an approach that has been shown to work. Mr Mukushi added that there is little evidence of the long-term impact of such a change. [36]

133. In his written evidence, Dr Garfield Benjamin indicates that it cannot be considered that consent is given for the use of facial recognition technology in public spaces, as this changes the role of the public and the police, saying that:

> "We must ask ourselves the cost, in terms of freedom, trust and inclusivity, of any surveillance technology. And we must not only regulate but develop and test such technologies according to the ethical and societal values we wish to embody".

134. In her written evidence, Dr Daly highlights public resistance to the trials by the Metropolitan Police Service and South Wales Police, as evidence that there is not public consent, and recommends a moratorium. [37]

135. Dr Lawless recommends that a public engagement exercise be undertaken to determine whether the public would give approval. Whilst, Dr Purshouse recommends a debate on the rules required to be in place and the limits of use, as well as research on the impact of the technology on individuals and society, be undertaken. [38]

136. In their written evidence, the Ada Lovelace Institute state that there should be an assurance of safeguards for the use of facial recognition technology by the police service, such as an appropriate form of public engagement, trials undertaken and an evidence base. [39]

137. In her submission, Dr Elizabeth Aston from Edinburgh Napier University, highlights that little is known of the impact on the legitimacy of the police service by introducing new technologies, and the willingness of people to comply and co-operate. Dr Aston suggests that:

> "As we would expect public opinion on the facial recognition software to be contentious it would be advisable for policing organisations to pause and agree not to proceed with its usage". [40]

138. The Sub-Committee considered whether people are able to give or withhold their consent for their biometrics data to be taken, when live facial recognition technology is used in a public space.

139. In her written submission, Gill Imery, Her Majesty's Chief Inspector of Constabulary, describes the use of live facial recognition technology as "controversial", saying that:

> "The reason that such technologies are so controversial is that they facilitate the instant capture of biometric data from members of the public sometimes without their knowledge or consent. This type of technology is capable of conducting mass screening surveillance of thousands of citizens and therefore potentially has profound consequences for privacy, data protection and human rights. It also raises a range of ethical concerns". [41]

140. Article 4(11) of the General Data Protection Regulation (GDPR) defines consent as: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

141. This requirement, as well as Section 35(2)(a) of the 2018 Act, led the UK Information Commissioner to conclude that it is "highly unlikely that individuals, including those not on a watchlist, will be able to provide valid consent for the processing of their biometric data for any of the law enforcement purposes where police use LFR in public spaces". [9]

142. T/ACC Sloan told the Sub-Committee that consent is an important issue for Police Scotland, especially when live facial recognition technology is used in circumstances where the public are not able to opt-out of their data being taken.

143. T/ACC Sloan explained that questions are being asked about the level of public engagement required, as a result of the trials in England and Wales. He indicated that if Police Scotland were to use live facial recognition technology in the future, they would need to explain to the public beforehand that they were using it for a strictly necessary and proportionate purpose. [42]

Impact on human behaviour

144. The Sub-Committee heard that live facial recognition technology had been trialled by police forces in England and Wales at events such as football matches, concerts, protests and marches.

145. Dr Purshouse told the Sub-Committee that its use at events has the potential to harm the relationship between the police and those attending, as well as heighten tensions amongst some groups, such as football fans.[xviii]

146. Recently published research,[xix] on the use of body-worn video cameras and hand-held cameras by the police service at football matches in Scotland found that "the use of technologies such as powerful hand-held cameras and body worn video (BWV) has had a detrimental impact on police-fan relationships, interactions and dialogue".

147. Some of those interviewed as part of the research project, described the process of being filmed at football matches as disproportionate, intimidatory, provocative, and counter-productive. The report concluded that:

> "Our findings also seem consistent with other research into Scottish policing, where attempting to improve police practices through imposing procedures that ignore the existing expertise and context-tailored approaches of frontline offices, can have surprisingly counter-intuitive and negative consequences."

148. Dr Diana Miranda from Northumbria University recently carried out research[xx] into the use of Body-Worn Video Cameras (BWVCs), which considered how these devices might be accompanied by other emerging technologies such as live facial recognition. The research consisted of interviews with police officers and explored some of the concerns that were discussed by officers when considering the potential use of live facial recognition.

149. Dr Miranda found that the views of police officers were mixed when it came to discussing the potential use of live facial recognition. Some officers were confident about the positive role that it could play in the future, while others were more sceptical about its use.

150. Some officers indicated that they were sceptical about the technical capabilities of the technology, and that they did not seem to trust a technology which is automated and dictated by non-human actors, such as computers. Officers also raised concerns about the accuracy of the technology and were not convinced that it was sufficiently robust at this point in time.

151. With regards to the use of live facial recognition in body-worn video cameras, concerns were raised about the prospect of constant filming, as this was seen as not being in the spirit of the use of BWVCs. It could also potentially harm the relationship between the police service and the public.

152. The Sub-Committee wrote[xxi] to Police Scotland on 19 December 2019, to seek clarification of whether body-worn video cameras, or any other equipment used by Police Scotland includes, or has the capability to use, facial recognition or facial matching technology.

153. In their response,[xxii] Police Scotland confirm that the body-worn video cameras that police officers use do not have facial recognition functionality. Police Scotland also

---

xviii Justice Sub-Committee on Policing, Official Report, 21 November, col 21

xix Lights, camera, provocation? Exploring experiences of surveillance in the policing of Scottish football, research by Niall Hamilton-Smith, University of Stirling, Maureen McBride, University of Glasgow, Colin Atkinson, University of the West of Scotland, published January 2020.

xx Dr Diana Miranda, Northumbria University, written submission, pages 1-8.

xxi Letter from the Justice Sub-Committee to Police Scotland, 19 December 2019.

confirm that they are currently considering national deployment of body-worn video cameras and that there is no expectation that the cameras will have facial recognition functionality.

154. Dr Lawless recommended that the police service should be "as open, precise and specific as possible about what they intend to use the technology for", if they intend to use facial recognition technology at public events.[xxiii]

155. Dr Bobak suggested that there may be public acceptance of the use of the technology in a targeted way, but not its indiscriminate use. Dr Bobak recommended the use of public information campaigns to ensure that the public are aware of exactly how the technology is to be deployed. [xxiv]

156. Griff Ferris indicated that the use of live facial recognition technology at public events, such as peaceful, democratic protests, could impact on "people's willingness or ability to exercise free expression". [xxv]

157. Matthew Rice described the effect on human behaviour of the use of live facial recognition technology as "chilling", explaining that:

> Not only surveillance that is overtly proven but people having the feeling that they are being watched can cause them to change their activities and behaviours.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 72[26]

158. T/ACC Sloan agreed that a tension exists between legitimate right to freedom of expression, which is a fundamental human right, and the police service's responsibility to keep people safe. He explained that:

> In order for the police to maintain public support, legitimacy and our relationship with the public, it is critical that there is significant consideration of how we would deploy the technology in public spaces. The biometrics commissioner and independent ethics groups should get round the table to explore and identify the issues and to find areas of commonality and consent.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 82[27]

159. T/ACC Sloan added that the debate on the use of new technologies is on-going. He told the Sub-Committee that the independent reference group, which is currently being established by the Scottish Government, will consider the use of facial recognition technology by the police.[xxvi]

160. Lynn Brown indicated that the SPA is to become a member of the Scottish Government's reference group, and that its work will provide reassurance about how technology will be taken forward. [xxvii]

---

xxii Police Scotland written submission, page 1.
xxiii Justice Sub-Committee on Policing, Official Report, 21 November, col 16
xxiv Justice Sub-Committee on Policing, Official Report, 21 November, col 16
xxv Justice Sub-Committee on Policing, Official Report, 5 December, col 18
xxvi Justice Sub-Committee on Policing, Official Report, 16 January, col 15
xxvii Justice Sub-Committee on Policing, Official Report, 16 January, col 15

Oversight and governance

Role of the Scottish Police Authority

161. The SPA has responsibility for governance, oversight and maintenance of the Police Service, for holding the Chief Constable to account, and for providing forensic services.

162. The 10-year policing strategy, Policing 2026, is a joint strategy between the SPA and Police Scotland. It includes plans to introduce a number of new technologies for use by Police Scotland, including facial recognition technology and cyber kiosks.

163. The issues that have been raised in evidence highlight a number of areas which require scrutiny prior to any decision to release funds to purchase live facial recognition technology. These issues are similar to those raised by the Sub-Committee in its report on its inquiry into Police Scotland's proposal to roll-out cyber kiosks to front-line police officers. A key issue within the report was a lack of oversight and scrutiny.

164. Police Scotland carried out operational trials of the kiosks without the consent or knowledge of the public and with a lack of oversight, scrutiny or impact assessments. The SPA did not carry out any analysis of the outcomes of the trials, or the implications for the public of the proposed changes to policing policy, before agreeing to procure the cyber kiosks.

165. There was also no public engagement and the legal basis for the use of cyber kiosks was not established.

166. In response to the Sub-Committee's inquiry, Police Scotland established a stakeholders' group and an external reference group to inform the development, direction and implementation of policy for cyber kiosks. These groups provided independent advice on human rights and data protection impact assessments, as well as consent. They also considered the legal basis for the introduction of the cyber kiosks.

167. In HMICS's report on its Thematic Inspection of the Scottish Police Authority, [2] the Inspectorate identified a number of key learning points for the SPA. These included that insufficient consideration had been given to human rights, equality and community impact assessment, and that there had been a lack of oversight.

168. Tatora Mukushi told the Sub-Committee that the 18-month delay in the deployment of cyber kiosks could have been averted if Police Scotland had carried out impact assessments. Mr Mukushi stated "That could have been averted by doing all the homework first, which would be an appropriate process to follow in this situation". [xxviii]

169. Matthew Rice suggested that the experience of trying to introduce the use of cyber kiosks should be used to inform the process and sequence of events, should live facial recognition technology be introduced. Mr Rice recommended that:

[xxviii] Justice Sub-Committee on Policing, Official Report, 5 December, col 12

> The public, members of the Scottish Parliament, civil society organisations and other groups should be able to feed into that before we even begin to think about procurement.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 56[28]

170. In her written evidence, Dr Aston referred to a lack of transparency and engagement by Police Scotland, saying that for cyber kiosks "inaccurate information was in the media and Police Scotland refused requests to engage in public fora on the issue". [xxix]

171. Dr Lawless told the Sub-Committee that the approach to the deployment of cyber kiosks had provided a learning opportunity, in terms of communicating with stakeholders and considering ethical issues before the technology is deployed.[xxx]

172. The UK Biometrics and Forensics Ethics Group in England and Wales outlined a framework of ethical principles that should be taken into consideration when developing policy on the use of live facial recognition technology for policing purposes. These include:

- "Public interest: The use of this technology is permissible only when it is being employed in the public interest.
- Effectiveness. The use of this technology can be justified only if it is an effective tool for identifying people.
- The Avoidance of Bias and Algorithmic Injustice: For the use of the technology to be legitimate it should not involve or exhibit undue bias. This can be unjust in two ways.
- Impartiality and Deployment. If the technology is deployed for policing purposes it must be used in an even-handed way. For example, it should not be used in ways that disproportionally target certain events, but not others, without a compelling justification.
- Necessity: such technology can be used only if other, less invasive, techniques are not available. Furthermore, the technology should be used in ways that minimize interference with people engaging in lawful behaviour.
- Proportionality: That is, it can be permissible only if the benefits are proportionate to any loss of liberty and privacy. The benefits have to be sufficiently great so as to justify any interference with other rights.
- Impartiality, Accountability, Oversight and the Construction of Watchlists.: If humans (or algorithms) are involved in the construction of watchlists for use with the technology, it is essential that they be impartial and free from bias. The construction of 'watchlists' needs to be subject to oversight by an independent body.

---

xxix Dr Elizabeth Aston, Edinburgh Napier University, written submission, page 2.
xxx Justice Sub-Committee on Policing, Official Report, 21 November, col 20

- Public Trust: it is important that those using it (either in operational deployments or trials) engage in public consultation and provide the rationale for its use.

- Cost-effectiveness. Any evaluation of the use of this technology needs to take into account whether any resources it requires could be better used elsewhere". [3]

173. Lynn Brown told the Sub-Committee that the SPA had learned lessons from its oversight of the proposal to introduce cyber kiosks, and that the experience had set out areas that needed to be considered by the police service prior to introducing new technology. Ms Brown added that "impact assessments around human rights and data should be common practice".[xxxi]

174. Ms Brown explained that the SPA's oversight of Policing 2026 would include a more structured approach to determining what is to be decided within the strategy, and would include working with external bodies, such as HMICS. Ms Brown confirmed that oversight would also include consideration of ethical concerns, stating that "We are acutely conscious that ethics is an area in which we should make sure that the public interest is served".[xxxii]

175. In response to a question about whether there is any conflict of interest for the SPA, in being a co-author of the 10-year strategy, and having responsibility for independent oversight of it, Ms Brown confirmed that Policing 2026 is the SPA's strategy. On the issue of the dual role of the SPA to maintain Police Scotland and to hold the Chief Constable to account, Ms Brown said:

> I know that the Auditor General for Scotland has said that maybe we should look at that, and the board is of the view that there definitely needs to be more clarity on that relationship and the various roles and responsibilities. We welcome that debate.
>
> Source: Justice Sub-Committee on Policing 16 January 2020 [Draft], Lynn Brown, contrib. 60[29]

Role of a Scottish Biometrics Commissioner

176. In its 2016 review, [1] HMICS recommended the establishment of an independent Scottish Commissioner to address issues of ethical and independent oversight of biometrics records and databases held in Scotland.

177. In response, the Scottish Government established the Independent Advisory Group on the Use of Biometric Data in Scotland (IAG). The IAG found that there was a need for strengthened governance and independent oversight. It recommended that there should be legislation to create an independent Scottish Biometrics Commissioner and a statutory Code of Practice. [12]

---

xxxi Justice Sub-Committee on Policing, Official Report, 16 January, col 9
xxxii Justice Sub-Committee on Policing, Official Report, 16 January, col 10

178. A Bill was introduced by the Scottish Government on 30 May 2019, and was being considered by the Scottish Parliament at the same time as the Sub-Committee was undertaking its inquiry into how policing in Scotland makes use of facial recognition technology.

179. During the Justice Committee's consideration of the general principles of the Scottish Biometrics Commissioner Bill, the possible introduction of the use of live facial recognition by Police Scotland was raised as a key concern by a number of stakeholders.

180. During its inquiry, the Sub-Committee heard views about the possible role, remit and priorities of a Scottish Biometrics Commissioner.

181. A number of witnesses recommended that Police Scotland's intention to introduce the use of live facial recognition technology should be a high priority for the Scottish Biometrics Commissioner.[xxxiii]

182. Tatora Mukushi told the Sub-Committee that the establishment of a legal framework, code of conduct, and clear guidance for the use of biometrics in policing should be prioritised. [xxxiv]

183. Griff Ferris stated that the Biometric Commissioner should consider whether live facial recognition technology should be used by the police service in Scotland at all. [xxxv]

184. Dr Ken Macdonald agreed that facial recognition should be included in the Commissioner's remit, but highlighted the need for clarity on the ICO's statutory role as the reserved regulator for data protection. [xxxvi]

185. Dr Purshouse recommended that the Biometric Commissioner's remit should cover the use of biometric surveillance for policing purposes by both the private and public sector. Dr Purshouse indicated that it will be important to ensure that terms such as "police purposes" are not interpreted too narrowly, to enable the Commissioner to express a view and regulate those activities. [xxxvii]

186. Dr Lawless told the Sub-Committee that a Biometrics Commissioner could play a role in verifying the claims made by software companies about the accuracy and effectiveness of their facial recognition software. [xxxviii]

187. In their written evidence, Police Scotland welcome proposals to establish a Scottish Biometrics Commissioner and a code of practice, and confirm that they will await the decision on the Bill currently before the Scottish Parliament before proceeding with any proposed use of facial recognition technology.[xxxix]

---

xxxiii Dr Purshouse, Dr Bobak, and Matthew Rice. Official Reports: 21 November 2019, col 17, and 5 December 2019, col 19.
xxxiv Justice Sub-Committee on Policing, Official Report 5 December, col 19
xxxv Justice Sub-Committee on Policing, 5 December, col 19
xxxvi Justice Sub-Committee on Policing, 5 December, cols 19-20
xxxvii Justice Sub-Committee on Policing, 21 November, col 18
xxxviii Justice Sub-Committee on Policing, 21 November, col 19
xxxix Police Scotland written submission, page 3.

188. In their submission, the SPA state that they agree with this approach. They also indicate that they expect Police Scotland to fully engage with the Authority and a future Scottish Biometrics Commissioner on any proposed use of such biometric technology. [page 1]

Moratorium

189. In July 2019, the UK Science and Technology Committee published a report on its inquiry into *Issues with biometrics and forensics significant risk to effective functioning of the criminal justice system*. The Committee called on the UK Government to issue a moratorium on the current use of automated facial recognition technology, saying that:

> "We reiterate our recommendation from our 2018 Report that automatic facial recognition should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved. We call on the Government to issue a moratorium on the current use of facial recognition technology and no further trials should take place until a legislative framework has been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established. [30]

190. It was reported by BBC News [43] on 20 January 2020, that the European Commission is considering a ban on the use of facial recognition in public areas for up to five years. They indicate that regulators want time to work out how to prevent the technology being abused. The Commission is considering introducing rules to strengthen existing privacy and data rights regulations, as well as imposing obligations on developers and users of artificial intelligence. It has urged EU countries to create an authority to monitor the new rules.

191. The need for a moratorium was expressed by a number of people and organisations,[xl] in their evidence to the Sub-Committee. Dr Purshouse recommended a moratorium on the use of live facial recognition until the following criteria are met:

> the case is made that there are clear uses for it, that the dangers of demographic bias have been properly mitigated and that it can be closely regulated so that its use is truly proportionate.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 26[31]

192. Tatora Mukushi told the Sub-Committee that if human rights and data protection standards cannot be built-into the design of the technology, it should not be introduced, saying that: "To be honest, if the technology cannot be developed with those things in place, that is a good argument for not using it". [xli]

---

xl The Open Rights Group, Big Brother Watch, the Scottish Human Rights Commission, Dr Joe Purshouse, University of East Anglia, Dr Liz Aston, Edinburgh Napier University, and Dr Birgit Schippers, St Mary's University College Belfast.

xli Justice Sub-Committee on Policing, Official Report, 5 December, col 16

193. Matthew Rice indicated that the technology should not be introduced without a proper legal framework and wide public debate. [xlii]

194. Dr Ken Macdonald referred to the need for a deletion process to be established to comply with data protection requirements, if images are to be processed. [xliii]

195. In her written evidence, Dr Elizabeth Aston recommended that there should be research and an informed debate prior to introducing the technology, saying that:

> "I would urge the Inquiry to recommend that a stop be put to any potential use of facial recognition software in Scotland until a thorough and lengthy process of evidence gathering, sharing of research, and a detailed informed public debate has been undertaken. This is in order that complex ethical, legal and societal concerns can be considered so that an informed decision can be taken as to the way forward for the public interest". [xliv]

196. The Sub-Committee received evidence highlighting decisions that have been made elsewhere to prohibit the use of live facial recognition technology.

197. In her written submission, Dr Angela Daly refers to the decision made to ban the technology in San Francisco, which has led to calls for a global moratorium on facial recognition technology for mass surveillance purposes.[xlv]

198. In his written evidence, Dr Garfield Benjamin highlights that Morocco has a moratorium on the use of facial recognition technology by the police service and that a broader moratorium bill is currently being considered in Massachusetts. [xlvi]

199. Dr Purshouse told the Sub-Committee that New Zealand is currently considering the appropriate parameters for the use of facial recognition surveillance and the extent to which there is a democratic mandate for its use, before making a decision on its use. Dr Purshouse provided the Sub-Committee with supplementary evidence of the preliminary findings of a research project he is involved in, which is looking at how the technology has been used and regulated in New Zealand. [xlvii]

200. The preliminary findings indicate that the Office of the Privacy Commissioner in New Zealand, responsible for monitoring the operation of New Zealand's Privacy Act 1993, is aware of potential harms arising from facial recognition technology, and has proactively developed a guidance document[xlviii] for agencies considering its use.

201. The New Zealand guidance lists a number of factors for those who wish to use facial recognition technology to consider. These include determining the lawful purpose for using the technology, considering how to notify people that you are

---

xlii Justice Sub-Committee on Policing, Official Report, 5 December, col 15
xliii Justice Sub-Committee on Policing, Official Report, 5 December, col 16
xliv Dr Elizabeth Aston, Edinburgh Napier University written submission, page 2.
xlv Dr Angela Daly, University of Strathclyde written submission, page 2.
xlvi Dr Garfield Benjamin, Solent University written submission, page 1.
xlvii Justice Sub-Committee on Policing, Official Report, 21 November, col 9

xlviii Office of the Privacy Commissioner, New Zealand.

using the technology, and whether the technology will be used in a way that might be unfair or unreasonably intrusive.

202. The New Zealand Privacy Commissioner also recommends that organisations considering collecting any personal information should undertake a privacy impact assessment.

Retrospective facial recognition technology

203. The Sub-Committee considered Police Scotland's current use of retrospective facial recognition technology, including facial search and match processes.

204. In their written evidence, Police Scotland outline their current use of retrospective facial recognition technology. They confirm that they upload criminal record images and intelligence to the UK Police National Database (PND), which has a facial matching functionality.[xlix]

205. A number of concerns were raised in evidence about Police Scotland's retention and use of photographic images, its use of the UK PND, and whether its processes are compliant with legislative requirements. These issues are considered below.

The legal basis for the retention and use of photographic images

206. In its 2016 review, HMICS found that the statutory framework in Scotland has specific legislation to govern and regulate the retention of biometrics such as fingerprints and DNA. However, there is no similar legislation which specifically governs the police retention and use of photographic images contained within Police Scotland's Criminal History System (CHS) or custody records.

207. HMICS recommended that the Scottish Government should work with Police Scotland and the SPA to consider legislative provision in relation to the retention and use of photographic images by the police, such as the development of a statutory code of practice for the use of biometric data in Scotland. [1]

208. In their written submission, HMICS indicate that this recommendation has not been implemented, and describe the legislative gap as "an ongoing risk requiring careful management".[l]

209. Included within the remit of the Independent Advisory Group on the Use of Biometric Data in Scotland (IAG), was a requirement to carry out a review of the retention of custody images[li] by Police Scotland. The IAG found that:

> "The absence of legislation in Scotland giving explicit authority to the police to take custody episode photographs is at variance with specific legislative authority in other parts of the UK". [12]

---

xlix Police Scotland, written submission, page 1.
l Her Majesty's Inspectorate of Constabulary in Scotland written submission, page 3.

210. Matthew Rice told the Sub-Committee that the lack of provision for the retention of facial images in the Criminal Procedure (Scotland) Act 1995, is at odds with the provisions available for retention of other data. Mr Rice explained that:

> That has led to divergence between practice on DNA—retention and deletion periods for which are quite clear—and practice in the situation with custody images that we are in.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice (Open Rights Group), contrib. 3[32]

211. In their joint written submission, the Open Rights Group and Big Brother Watch state that the use of post-event facial recognition analysis "must be provided for by law". They call on the Scottish Parliament to clarify the legal basis for the police service taking and retaining images.[lii]

212. Dr Ken Macdonald agreed that legislative measures which clarify retention and disposal periods would be welcome, but cautioned that Police Scotland's legacy IT systems were not designed to meet current data protection and privacy requirements. Dr Macdonald indicated that the systems only offered the option of wholesale deletion of images, which in his view, would not be pragmatic. [liii]

213. T/ACC Sloan told the Sub-Committee that the 1995 Act, specifies retention of DNA samples, but is less clear in relation to retention of images.

214. In response to a question about whether it would be helpful if the 1995 Act were to be updated to cover photographs and images, T/ACC Sloan replied "absolutely". He added that "a framework and guidance that would allow us [Police Scotland] to operate within it would be valued and welcomed".[liv]

215. In January 2017, Police Scotland introduced a new national custody solution to consistently manage custody episodes.

216. The IAG found that Police Scotland currently holds or retains more than 1 million custody images, and that the new system should have the technical capability to identify and dispose of photographs of people who are not convicted or not proceeded against.

217. However, the IAG states that Police Scotland has not changed its policies on custody image retention. They noted that a legislatively mandated weeding regime "would require Police Scotland to consider a policy, process and technical response to ensure compliance within an acceptable timeframe in relation to the legacy custody applications". [12]

218. In their joint written submission, the Open Rights Group and Big Brother Watch raise a concern that Police Scotland is retaining images on its systems that were taken prior to them introducing a policy in 2017 to remove images after 6 months. They indicate that, in March 2018, Police Scotland held over a million custody

---

li Custody image – a photograph of an individual taken when processed at a police office as a suspect or accused person.
lii Open Rights Group and Big Brother Watch joint written submission, pages 2-3.
liii Justice Sub-Committee on Policing, Official Report, 5 December, col 2
liv Justice Sub-Committee on Policing, Official Report, 16 January, cols 4-5

images. The Open Rights Group and Big Brother Watch recommend that Police Scotland, "immediately remove all historic images of unconvicted people from the Criminal History System and Police National Database". [lv]

219. T/ACC Sloan confirmed that images of innocent people are retained on Police Scotland's legacy IT systems, and that they are "working towards a situation in which no images will be held anywhere other than the criminal history system".[lvi]

220. T/ACC Sloan stated that, in the absence of legislation or a guidance framework for the retention of images, Police Scotland voluntarily deletes images at the same point as it deletes DNA and fingerprints. [lvii]

221. The Sub-Committee notes that the Justice Committee recommended in its Stage 1 report on the Scottish Biometrics Commissioner Bill that the Scottish Government work with Police Scotland and the SPA to consider legislative provision in relation to the retention and use of photographic images by the police. As this represents a legislative gap. [33]

222. The Scottish Government indicated in its response to the Committee's Stage 1 report, that it:

> "will consider the need for legislation regarding retention periods for images as part of the review that it has already committed to undertake in respect of the current law on retention periods for biometric data more widely".[lviii]

Use of the UK Police National Database

223. The UK PND was introduced in 2008. It is provided, and approved, by the Home Office. It enables all UK police forces to upload an individual image of a suspect, and to use its facial search software to compare that image against others held on file.

224. In their written evidence, Police Scotland confirm that they uploaded all of the records and images from their Criminal History System to the PND in 2011. They also confirm that in March 2014, the Home Office introduced a UK-wide facial search functionality within the Database, and that no privacy impact assessment was conducted on it after 2013.[lix]

225. T/ACC Sloan told the Sub-Committee that Police Scotland's current practice is to upload a photograph to their national custody system when an individual is taken into custody, arrested and charged. That photograph is then transferred to the Criminal History System, and uploaded to the PND.[lx]

---

lv Open Rights Group and Big Brother Watch joint written submission, pages 2-3.
lvi Justice Sub-Committee on Policing, Official Report, 16 January, col 6
lvii Justice Sub-Committee on Policing, Official Report, 16 January, col 4
lviii Scottish Government's response to the Justice Committee's Stage 1 report on the Scottish Biometrics Commissioner Bill, page 5.
lix Police Scotland written submission, page 1.
lx Justice Sub-Committee on Policing, Official Report, 16 January, col 2

226. If the person is found not guilty, notification is passed to the police records bureau, and images are deleted from the CHS. Images are then deleted from the PND, "as near to simultaneously as possible, when results come in". T/ACC Sloan added that other types of images retained by Police Scotland, such as those from CCTV or body-worn video cameras, or on legacy systems, are not uploaded or stored on the PND. He explained that this is because only images that are contained on the CHS are uploaded, and images that have been retained from legacy forces are held on separate systems.[lxi]

227. In supplementary evidence, T/ACC Sloan confirmed that "no images from legacy IT systems, CCTV, mobiles, etc. are uploaded to PND by Police Scotland".[lxii]

228. In January 2016, HMICS published an Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland. The review considered Police Scotland's use of the Criminal History System, and the UK PND.

229. HMICS found that Police Scotland had made "very limited and selective use of this PND functionality" and were satisfied that their use of its facial search was appropriate. However, the Inspectorate raised a specific concern about a lack of oversight, finding that:

> "Whilst noting the statutory responsibilities of the Scottish Police Authority (SPA) to hold the Chief Constable to account for the policing of Scotland, we are unaware of any specific work in Scotland that has sought to provide external assurance over the use of PND by Police Scotland". [1]

230. Griff Ferris told the Sub-Committee that "there are 21 million images in the [Police National] Database, and 12 million of those have been made searchable by facial recognition technology". Mr Ferris added that the Home Office is currently reviewing all of the images in order to decide whether they can be deleted. [lxiii]

231. In their 2016 review, HMICS found that the introduction of the facial matching functionality provided the ability to search third-party sourced images of suspects (known as probe images) against that database. This included images sourced from CCTV, mobile telephones, or police body-worn video cameras. [1]

Compliance with human rights and data protection legislation

232. The Sub-Committee considered whether Police Scotland's use of retrospective facial recognition technology is compliant with human rights legislation.

233. In its 2016 review, HMICS found that there is no legislation in England and Wales specific to the police retention and use of photographic images, meaning that most are retained indefinitely. [1]

---

lxi Justice Sub-Committee on Policing, Official Report, 16 January, cols 3, 5 and 16
lxii Police Scotland, supplementary written evidence, page 1.
lxiii Justice Sub-Committee on Policing, Official Report, 5 December, col 3

234. In their written evidence, HMICS describe the PND as "controversial", as police forces in England and Wales have not removed records of those not subsequently proceeded against or convicted, stating that:

> "The consequence is that the UK PND contains thousands of images of innocent persons. This has attracted extensive criticism including from the UK Commissioner for the Retention and Use of Biometric Data". [1]

235. The IAG found that Police Scotland only upload images to the PND of those who had been charged with a crime or offence. However, in England and Wales, most forces upload all custody images directly to the Database. The Group found that questions remain about the proportionality, effectiveness and efficiency of current biometric data retention regimes in Scotland. It stated that the "absence of specific legislative authority for the police to capture custody episode images raises important human rights concerns". The lack of regulation was particularly concerning in respect to children and vulnerable individuals. [12]

236. In their joint submission, the Open Rights Group and Big Brother Watch highlight a court ruling in 2012 which found that "indefinite retention of innocent people's custody images was "unlawful".[lxiv]

237. Dr Bobak told the Sub-Committee that there are technical issues with deleting the images held on the PND, which means that despite the court ruling, this issue remains unresolved. [lxv]

238. Dr Purshouse told the Sub-Committee that the UK PND contains hundreds of thousands, if not millions, of custody images of people who were arrested, but not convicted of an offence. Dr Purshouse explained that the Home Office had tried to resolve that issue by implementing a policy that anyone who had not been convicted could apply to have their image taken off the PND. However, the policy was not widely publicised, and therefore the take-up of that option is very low. [lxvi]

239. Dr Purshouse explained that this intrusion of privacy rights makes it necessary for Police Scotland to satisfy itself that it is not accessing and using images of innocent people. He said that:

> It is important that Police Scotland is aware of that and that a system is in place to manage whether Police Scotland can have access to, or potentially use, images that have been stored latently in a facial recognition system long after someone was involved in a criminal process but was not convicted.
>
> Source: Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 45[34]

240. Tatora Mukushi explained that using images of people who have not been convicted of any crime engages Article 8 rights,[lxvii] and could engage Article 6 rights[lxviii] of the European Convention of Human Rights (ECHR). Mr Mukushi stated that this leaves the police service open to legal challenge and that it may not meet the standard for the admissibility of evidence, saying that:

---

lxiv Open Rights Group and Big Brother Watch joint written submission, pages 5 and 6.
lxv Justice Sub-Committee on Policing, Official Report, 21 November, col 14
lxvi Justice Sub-Committee on Policing, Official Report, 21 November, col 12
lxvii [1] ECHR Article 8: Respect for your private and family life.

> If it was known that the police had used faulty or unlawfully held images in identifying suspects, or in any part of an investigation, that investigation would then be suspect.
>
> Source: Justice Sub-Committee on Policing 05 December 2019 [Draft], Tatora Mukushi, contrib. 16[35]

241. Dr Lawless indicated that there could be a legal challenge or appeal if Police Scotland matched someone whose image was retained on the UK PND, despite them being innocent of any crime. Dr Lawless recommended that there should be a consistent approach applied to the retention of biometrics, with "a retention regime similar to that for DNA" for Scotland, England and Wales.[lxix]

242. T/ACC Sloan confirmed that Police Scotland "could come across an image of a person who was not convicted— who was innocent", whilst utilising the UK PND. He indicated that this prospect "creates a concern nationally", given the 2012 court ruling[lxx] which found that it is illegal to hold such images. [lxxi]

243. The Sub-Committee also heard that watchlists are compiled from images and can be used for both live and retrospective facial recognition and matching. Concerns were raised in evidence about the inclusion of people on these lists who had not been convicted of a crime.

244. In her published Opinion, the UK Information Commissioner said that it would be less likely that images of those who are wanted or suspected of non-serious offences contained on watchlists would meet the 'strict necessity' data protection threshold. Ms Denham also raised "significant concerns" about watchlists which are compiled using custody images that should have been deleted from police systems, as "these individuals are not charged with an offence or are charged but not convicted". [9]

Private companies and public sector agencies supplying images to Police Scotland

245. Police Scotland's 10-year strategy, Policing 2026, indicates their intention to access and share facial recognition data with other public sector agencies, as well as private companies. The Sub-Committee heard that there are data protection, human rights and privacy concerns, regarding this proposal.

---

lxviii [2] ECHR Article 6: Right to a fair trial.

lxix Justice Sub-Committee on Policing, Official Report, 21 November, col 13

lxx In 2012 the High Court held that the governance framework then used by the police was not proportionate in its retention rules and as such was unlawful. The court drew attention to the 'risk of stigmatisation of those entitled to the presumption of innocence' and that holding images of those unconvicted for a long period (a minimum of 6 years) was not proportionate. They added that retaining images in such cases for minors would be especially harmful. https://www.gov.uk/government/news/response-to-the-home-office-review-of-the-retention-and-use-of-custody-images

lxxi Justice Sub-Committee on Policing, Official Report, 16 January, col 5

246. In their joint submission, the Open Rights Group and Big Brother Watch (BBW) refer to an investigation undertaken by BBW, which found that numerous private companies in England and Wales were using facial recognition. The investigation also found that there were partnerships between police forces and private companies, for example, between the Metropolitan Police Service, the British Transport Police and the Kings Cross Estate Development company [44] in central London. [lxxii]

247. Griff Ferris described the lack of transparency in these partnerships as "extremely concerning". Mr Ferris explained that a lack of safeguards enabled private companies to use facial recognition secretly without being held to the same high standards as public authorities.[lxxiii]

248. Tatora Mukushi told the Sub-Committee that, given the intrusion into people's lives, private companies who provide data to a public authority, such as images, should have to meet the same human rights requirements as the public authority. Mr Mukushi recommended that the Scottish Government shouldn"… say that any organisation that uses biometric data should be held to a higher standard, because of the nature of biometric data".[lxxiv]

249. Matthew Rice recommended that legislation should cover information being provided, viewed and shared with Police Scotland by an external organisation. Mr Rice gave the example of Glasgow City Council providing Police Scotland with access to its CCTV system. This specific example is covered in more detail later in this report. [lxxv]

250. Dr Ken Macdonald told the Sub-Committee that there are concerns about where the relationship between the police and private companies fits within the GDPR regime. Dr Macdonald explained that "there needs to be a clear contract between the two parties, especially when a party acts as processor on behalf of the police". [lxxvi]

251. In their Stage 1 report on the Scottish Biometrics Commissioner Bill, the Justice Committee recommended that the Scottish Government consult on whether other public sector bodies should be included within the scope of the Bill. The Committee also asked for details of how the Commissioner is expected to assess the scope of biometrics being used for criminal justice and policing purposes in Scotland, which are provided by the private sector, and the oversight regime required to achieve this. **33**

252. In their response, the Scottish Government indicate that they would consider undertaking a consultation, "once sufficient time has passed, to allow the current oversight provisions to bed in". They also confirmed that private sector companies "would not currently be subject to direct formal oversight by the Commissioner".

---

lxxii Open Rights Group and Big Brother Watch joint written submission, page 4.
lxxiii Justice Sub-Committee on Policing, Official Report, 5 December, col 20
lxxiv Justice Sub-Committee on Policing, Official Report, 5 December, col 22
lxxv Justice Sub-Committee on Policing, Official Report, 5 December, col 21
lxxvi Justice Sub-Committee on Policing, Official Report, 5 December, col 23

253. The Scottish Government added that the Scottish Biometric Commissioner's code of practice could make recommendations about when or how bodies in section 2(1) of the Bill enter into contracts with private sector bodies and what assurances should be given in those contracts. [lxxvii]

Glasgow City Council CCTV system – Suspect Search

254. The Sub-Committee considered Glasgow City Council's intention to introduce software called 'Suspect Search' into its public space CCTV system, and to provide Police Scotland with access to the data it collects and creates.

255. The Sub-Committee wrote[lxxviii] to Glasgow City Council to request information on media reports of its plans to upgrade its CCTV system to include Suspect Search. Reports indicated that the software has the capability to locate and track individuals, for example, by uploading a photograph. The Sub-Committee also sought confirmation of the type of information that would be shared with Police Scotland.

256. Glasgow City Council confirm in their response that their CCTV system was upgraded in 2014, to include Suspect Search software (renamed Person Search for Glasgow), and that the software has not been used to date. They also confirm that the software is not based on facial recognition, but on characteristics, such as full body image, and that it includes a "quasi-real time" tracking functionality. Glasgow City Council describe the image matching process, as follows:

"1. Select a reference image/person by retrieving a person's image from the CCTV system (if seen on camera)

2. Upload a photo of the person (e.g. a missing person) - this becomes the reference image

3. Create an image with the built-in composite tool (known as an avatar)".[lxxix]

257. Glasgow City Council confirm that Police Scotland will be able to access the Suspect Search technology. They acknowledge that this access could breach the human rights of those whose images are inadvertently captured as "collateral intrusion".[lxxx]

258. They explain that Police Scotland can use the software for pre-planned or planned purposes, and there are different processes and safeguards applied to each.

259. Pre-planned use would require to be authorised in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") and authorised by Glasgow City Council's Investigations Manager, in accordance with their policy and guidelines on directed surveillance.

---

lxxvii Scottish Government's response to the Justice Committee's Stage 1 report on the Scottish Biometrics Commissioner Bill, page 8.
lxxviii Letter from the Justice Sub-Committee on Policing to Glasgow City Council, 4 October 2019.
lxxix Letter from Glasgow City Council to the Justice Sub-Committee on Policing, page 1.
lxxx Letter from Glasgow City Council to the Justice Sub-Committee on Policing, page 2.

260. Authorisation would be for the purpose of preventing or detecting crime or of preventing disorder; in the interests of public safety; or for the purpose of protecting public health.

261. Unplanned use, for example to locate someone being sought in connection with a real-time incident, would not require prior authorisation.

262. Glasgow City Council are awaiting the approval of a Data Protection Impact Assessment (DPIA), both internally and by the UK Information Commissioner's Office, prior to commencing operational use of the system.

263. In March 2019, the Surveillance Camera Commissioner in England and Wales issued guidance [36] to relevant English and Welsh authorities on the overt operation of surveillance camera systems in public places, including those which make use of automated facial recognition technology (AFR).

264. The Surveillance Camera Commissioner made a number of recommendations, which include:

- the need for a relevant authority to be clear and transparent as to the legal basis upon which they seek to rely to justify the use of AFR;
- providing clarity on why it is considered necessary to use the intrusive capabilities of AFR in such circumstances rather than simply desirable, and
- that decisions over the deployment of the most appropriate technology should be proportionate to the stated purpose rather than driven by its availability.

265. The relevant authority should also complete a detailed risk assessment to document the operational, community impact, privacy, human rights, and any other risks.

266. In their joint submission, the Open Rights Group and Big Brother Watch highlight that Glasgow City Council's proposed introduction of Suspect Search "raises the question of a private or public sector body deploying surveillance technology that Police Scotland subsequently have access to or rely on". [lxxxi]

267. In their written evidence, the Law Society of Scotland indicate that section 163 of the Criminal Justice and Public Order Act 1994, provides an important safeguard against disproportionate intrusion of the use of facial recognition technology, as "the local controllers of CCTV systems would need to be satisfied that the police had a genuine reason for accessing footage". [lxxxii]

268. In their 2016 review, HMICS recommended that statutory codes of practice on biometrics for the wider public sector would establish clearly understood principles and safeguards for the public, such as biometric data held by other public agencies, for example CCTV records and databases. [1]

269. In their Stage 1 consideration of the Scottish Biometrics Commissioner Bill, the Justice Committee asked the Scottish Government to review the scope of the

---

lxxxi Open Rights Group and Big Brother Watch joint written submission, page 15.
lxxxii The Law Society of Scotland written submission, page 4.

Commissioner's remit and powers. The Committee recommended that the review include a consultation on whether other public sector bodies should be included within the scope of the Bill, for example local government CCTV systems. [33]

270. In their response, the Scottish Government indicate that: "it may be appropriate in future to extend the Commissioner's oversight role to cover other criminal justice-related matters".[lxxxiii]

lxxxiii Scottish Government's response to the Justice Committee's Stage 1 report on the Scottish Biometrics Commissioner Bill.

Conclusions and recommendations

Live facial recognition technology

271. Police Scotland does not currently use live facial recognition technology. However, at present plans to introduce facial recognition technology are included in Police Scotland's 10-year strategy, Policing 2026.

272. The evidence received by the Sub-Committee during its inquiry indicates that a number of safeguards need to be met, prior to Police Scotland introducing the use of this technology. A key issue to be resolved is the technology's lack of accuracy.

273. It is clear that live facial recognition technology is currently not fit for use by Police Scotland. The Sub-Committee believes that there would be no justifiable basis for Police Scotland to invest in technology which is known to have in-built racial and gender bias, and unacceptably high levels of inaccuracy.

274. The Sub-Committee therefore welcomes Police Scotland's confirmation that they will not introduce live facial recognition technology at this time. We also welcome their commitment to participate in a wider debate on policy, which will include civil liberties groups and academics, and to ensure that necessary safeguards are in place, prior to making any decision to introduce live facial recognition technology. Wide stakeholder engagement has clearly added value to current plans to deploy cyber kiosks.

275. However, if Police Scotland does not now intend to introduce live facial recognition technology by 2026, the Scottish Police Authority should update the 10-year strategy to reflect that position, as part of the planned review in 2020.

276. If Police Scotland does intend to introduce live facial recognition technology at some point in the future, the impact of its use must be fully understood prior to any decision being taken to introduce it to policing in Scotland.

277. The recent challenges in court to the legality of the use of live facial recognition technology by the police services in England and Wales suggests that there is a lack of public consent for its use, as well as a lack of confidence in the current legal framework being relied upon.

278. The Sub-Committee recommends that the following actions be taken prior to any decision to introduce live facial recognition technology to policing in Scotland:

- The Policing 2026 strategy should be updated to include details of the type of technology to be introduced, and the necessity and parameters of its use. The strategy's equality and human rights impact assessment (EqHRIA) should also be reviewed by the Scottish Police Authority to ensure that it is suitably robust.
- The Scottish Police Authority must ensure that comprehensive human rights, equalities, community impact, data protection and security assessments are carried out.

- Similar assessments are also required prior to introducing any other technologies within Policing 2026, especially where there is a risk of collateral intrusion into areas of personal privacy and human rights. Any such assessments should be made publicly available.

- The Cabinet Secretary for Justice must ensure that there is a robust legal and regulatory basis for the use of live facial recognition technology in Scotland. This would provide legitimacy for the police service and assurance for the public. The Sub-Committee requests clarification of the Government's plans, and whether this would include a consultation on public consent for the use of this technology.

- The Scottish Police Authority must review the legal challenges to the use of live facial recognition technology by police forces in England and Wales, and consider how to mitigate the risk of similar legal challenges in Scotland.

- The Sub-Committee has not received sufficient evidence of the necessity to introduce live facial recognition technology, or that it is possible to use it in a proportionate way. Its use on people who attend legitimate and legal pursuits, such as peaceful protests, concerts or sporting events, is not necessary or proportionate. The Scottish Police Authority should assess the necessity, proportionality and parameters of its use.

- Police Scotland needs to demonstrate that there is public consent for the use of live facial recognition technology before introducing it, as a lack of public consent risks undermining the legitimacy of the technology and potentially, public confidence in policing. It could also represent a failure to meet the principles set out in the Police and Fire Reform (Scotland) Act 2012.

- Any consultation on the introduction of the use of live facial recognition technology must take into consideration its potential impact on human behaviour and the relationship between the public and the police.

- Police Scotland and the Scottish Police Authority must clarify how they will ensure that data protection requirements will be met for the use of live facial recognition technology. This should include confirmation of whether a data protection impact assessment detailing the risks and how these are to be mitigated would be a necessary requirement.

- The Scottish Police Authority should take account of the UK Biometrics and Forensics Ethics Group's framework of ethical principles when considering Police Scotland’s proposal to introduce the use of live facial recognition technology.

- To provide public confidence, any incoming Scottish Biometrics Commissioner should consider any future plans by Police Scotland to introduce the use of live facial recognition technology prior to a decision being taken by the Scottish Police Authority to approve its introduction.

Retrospective facial recognition technology

279. Police Scotland currently use retrospective facial recognition technology, which includes facial search and match processes.

280. The Sub-Committee heard concerns about the legal basis for Police Scotland's use of retrospective facial technology, and whether their processes meet human rights and data protection requirements.

281. The lack of legislation enabling Police Scotland to retain and use photographic images held on its IT systems is an issue which must be addressed.

282. Police Scotland's retention and use of images of innocent people held on its legacy IT systems and on the UK Police National Database, is another issue which must be addressed.

283. This practice infringes the human rights of those whose images are retained and represents an ongoing risk of both legal challenge and reputational damage to Police Scotland.

284. The Sub-Committee is concerned about the lack of regulation and transparency over the use of facial recognition technology by private companies and in the wider public sector, and their practice of sharing the data they collect with the police service. If the Scottish Biometrics Commissioner is not to have any formal oversight of the private sector or wider public sector, they will not be held to the same standard as the police service.

285. The Sub-Committee recommends that the following actions be taken to address concerns about Police Scotland's use of retrospective facial recognition technology:

- The Scottish Government should confirm whether it will legislate to enable Police Scotland to take, retain, use and share photographic images.
- The Scottish Government should address the lack of regulation over the use of facial recognition technology by private companies, and by the wider public sector, and the data they share with the police service.
- Police Scotland should to provide details of its plans, including the timescale, for deleting images of innocent people retained on legacy databases.
- The Scottish Police Authority should carry out a review of Police Scotland's use of retrospective facial recognition technology. This should include their use of the UK Police National Database and the legal basis for uploading photographs to that database. It should also include consideration of the consequences of their access to and use of any images of innocent people held illegally on that Database. The review should take a human rights-based approach to this assessment.

286. During its inquiry, the Sub-Committee considered Glasgow City Council's plans to introduce 'Suspect Search' software into its public space CCTV system, and to provide Police Scotland with access to the data it collects and creates.

287. Glasgow City Council confirmed in their written evidence that the software is not based on facial recognition, but on characteristics, such as full body image. They also confirmed that it has a tracking functionality, which is described as "quasi-real time", to reflect the time delay in tracking an individual.

288. The software has not yet been introduced, as the UK Information Commissioner's Office is currently considering the data protection impact assessment. The Sub-Committee is to write to the ICO to request an update on its consideration, and to Glasgow City Council to request further details of its plans.

289. The Sub-Committee asks the Scottish Police Authority to review Police Scotland's plans to access and use Glasgow City Council's Suspect Search technology. This should include consideration of whether all the necessary impact assessments have been undertaken and safeguards met.

Annex

The Sub-Committee took oral evidence at the following meetings-

- Thursday 21 November 2019: Minutes and Official Report
- Thursday 5 December 2019: Minutes and Official Report
- Thursday 16 January 2020: Minutes and Official Report

The Sub-Committee received written submissions from-

- Ada Lovelace Institute
- Dr Elizabeth Aston, Edinburgh Napier University
- Dr Garfield Benjamin, Solent University
- Big Brother Watch and Open Rights Group
- British Transport Police
- Crown Office and Procurator Fiscal Service
- Dr Angela Daly, University of Strathclyde
- Brian Griffiths
- Glasgow City Council
- Her Majesty's Inspectorate of Constabulary in Scotland (HMICS)
- Information Commissioner's Office
- Law Society of Scotland
- Dr Christopher Lawless, Durham University
- Liberty
- Dr Diana Miranda, Northumbria University
- NO2ID
- Jessie Normaschild
- Police Scotland
- Privacy International
- Dr Joe Purshouse, University of East Anglia, Professor Liz Campbell, Monash University, Dr Marcin Betkier and Dr Nessa Lynch, Victoria University of Wellington
- Dr Kay Ritchie, University of Lincoln and Dr David White, UNSW Sydney

- Dr Birgit Schippers, St Mary's University College Belfast
- Scottish Human Rights Commission
- Scottish Police Authority
- Scottish Police Federation
- Alistair Sloan, Inksters Solicitors
- Gregor Szczesny

The Sub-Committee received supplementary written submissions from-

- Big Brother Watch
- British Transport Police
- Dr Diana Miranda, Northumbria University
- Dr Joe Purshouse, University of East Anglia, Professor Liz Campbell, Monash University, Dr Marcin Betkier and Dr Nessa Lynch, Victoria University of Wellington
- Police Scotland

[1] Her Majesty's Inspectorate of Constabulary in Scotland. (2016, January). Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland. Retrieved from https://www.hmics.scot/sites/default/files/publications/HMICS%20Audit%20and%20Assurance%20Review%20of%20the%20use%20of%20the%20Facial%20Search%20functionality%20within%20the%20UK%20Police%20National%20Database%20%28PND%29%20by%20Police%20Scotland_0.pdf

[2] Her Majesty's Inspectorate of Constabulary in Scotland. (2019, September). Thematic Inspection of the Scottish Police Authority. Retrieved from https://www.hmics.scot/sites/default/files/publications/HMICS20190926PUB.pdf

[3] UK Biometrics and Forensics Ethics Group in England and Wales. (n.d.) Ethical issues arising from the police use of live facial recognition technology. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf

[4] Police Scotland and the Scottish Police Authority. (2017, June 20). Policing 2026: Serving a Changing Scotland. Retrieved from https://www.scotland.police.uk/assets/pdf/138327/386688/policing-2026-strategy.pdf

[5] Police Scotland and the Scottish Police Authority. (2018, March 9). Equality and Human Rights Impact Assessment (EqHRIA) Summary of Results. Retrieved from https://www.scotland.police.uk/assets/pdf/459397/2026-eqhria-summary-of-results?view=Standard

[6] Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 5, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219713

[7] Justice Sub-Committee on Policing 21 November 2019, Dr Christopher Lawless (Durham University), contrib. 7, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219715

[8] Judgement in the case of R (on the application of Bridges) v Chief Constable of South Wales Police. (2019, September 4). Retrieved from https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

[9] UK Information Commissioner. (2019, October 31). Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places. Retrieved from https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/LFR_opinion_pdf.pdf

[10] Justice Sub-Committee on Policing 05 December 2019 [Draft], Dr Macdonald, contrib. 19, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224308

[11] Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 21, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224310

[12] Independent Advisory Group (IAG) on the Use of Biometric Data in Scotland. (2018, March 22). Use of biometric data: report of the independent advisory group. Retrieved from https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/

[13] Ada Lovelace Institute. (2019, September). Beyond face value: public attitudes to facial recognition technology. Retrieved from https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

[14] Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 84, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219792

[15] Justice Sub-Committee on Policing 21 November 2019, Dr Bobak, contrib. 85, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219793

[16] Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 44, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230915

[17] Justice Sub-Committee on Policing 16 January 2020 [Draft], Lynn Brown (Scottish Police Authority), contrib. 48, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230919

[18] Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 46, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224335

[19] Justice Sub-Committee on Policing 05 December 2019 [Draft], Griff Ferris, contrib. 20, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224309

[20] Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 46, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230917

[21] Justice Sub-Committee on Policing 16 January 2020 [Draft], Tom Nelson (Scottish Police Authority), contrib. 68, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230939

[22] Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 11, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219719

[23] Justice Sub-Committee on Policing 05 December 2019 [Draft], Griff Ferris, contrib. 28, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224317

[24] Justice Sub-Committee on Policing 05 December 2019 [Draft], Tatora Mukushi, contrib. 37, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224326

[25] Justice Sub-Committee on Policing 05 December 2019 [Draft], Dr Macdonald, contrib. 23, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224312

[26] Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 72, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224361

[27] Justice Sub-Committee on Policing 16 January 2020 [Draft], Temporary Assistant Chief Constable Sloan, contrib. 82, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230953

[28] Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice, contrib. 56, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224345

[29] Justice Sub-Committee on Policing 16 January 2020 [Draft], Lynn Brown, contrib. 60, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12462&c=2230931

[30] The House of Commons Science and Technology Committee. (2019, July 18). Issues with biometrics and forensics significant risk to effective functioning of the criminal justice system. Retrieved from https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/biometrics-commissioner-forensic-science-regulator-report-publication-17-19/

[31] Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 26, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219734

[32] Justice Sub-Committee on Policing 05 December 2019 [Draft], Matthew Rice (Open Rights Group), contrib. 3, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224292

[33] Scottish Parliament Justice Committee. (9, December 2019). Stage 1 report on the Scottish Biometrics Commissioner Bill. Retrieved from https://digitalpublications.parliament.scot/Committees/Report/J/2019/12/9/Scottish-Biometrics-Commissioner-Bill-Stage-1-Report#INTRODUCTION

[34] Justice Sub-Committee on Policing 21 November 2019, Dr Purshouse, contrib. 45, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12389&c=2219753

[35] Justice Sub-Committee on Policing 05 December 2019 [Draft], Tatora Mukushi, contrib. 16, http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=12420&c=2224305

[36] Surveillance Camera Commissioner. (2019, March). The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf

1 Official Reports: 21 November 2019, 5 December 2019, and 16 January 2020.

2 Police Scotland written submission, page 2

3 Police Scotland written submission, pages 2-3

4 Scottish Police Federation written submission, pages 1 and 3

5 Liberty written submission, page 1

6 Joint Open Rights Group and Big Brother Watch written submission, page 3

7 Ada Lovelace Institute written submission, page 3

8 Liberty written submission, page 2

9 Liberty written submission, page 6

10 Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks), page 8.

11 Law Society of Scotland written submission, page 5

12 Justice Sub-Committee Official Report, 21 November 2019, Col 4

13 Justice Sub-Committee Official Report, 21 November 2019, Cols 7-8

14 Police Scotland written submission, page 3

15 Her Majesty's Inspectorate of Constabulary in Scotland written submission, page 3

16 Crown Office and Procurator Fiscal Service written submission, page 1

17 Justice Sub-Committee, Official Report 21 November 2019, col 15

18 Dr Angela Daly, University of Strathclyde Law School written submission, page 2

19 Justice Sub-Committee, Official Report 21 November 2019, col 6

20 Justice Sub-Committee, Official Report, 16 January 2020, col 8

21 Justice Sub-Committee Official Report, 21 November 2010, col 10

22 Justice Sub-Committee Official Report, 5 December 2019 col 12

23 Justice Sub-Committee Official Report, 5 December 2019, cols 12-13

24 Dr Angela Daly University of Strathclyde Law School written submission, page 1

25 Justice Sub-Committee Official Report, 5 December, cols 23-24

26 Law Society of Scotland written submission, page 3

27 Justice Sub-Committee Official Report, 5 December, cols 14-15

28 Justice Sub-Committee Official Report, 5 December, col 13

29 Justice Sub-Committee Official Report, 16 January, cols 10-12

30 Justice Sub-Committee Official Report, 16 January, col 12

31 Justice Sub-Committee Official Report, 21 November, cols 9-12

32 Justice Sub-Committee Official Report, 21 November, cols 11 and 17

33 Justice Sub-Committee Official Report, 16 January, col 13

34 Justice Sub-Committee Official Report, 16 January, cols 12-13

35 Crown Office and Procurator Fiscal Service written submission, page 1.

36 Justice Sub-Committee on Policing, Official Report, 5 December col 17

37 Dr Angela Daly, University of Strathclyde, written submission, pages 1 and 2

38 Justice Sub-Committee on Policing, Official Report, 21 November, cols 6-7

39 The Ada Lovelace Institute, written submission, page 2

40 Dr Elizabeth Aston, Edinburgh Napier University, written submission, page 1

41 Her Majesty's Inspectorate of Constabulary in Scotland, written submission, page 1

42 Justice Sub-Committee on Policing, Official Report, 16 January, col 14

43 BBC News: Facial recognition: EU considers ban of up to five years.

44 Kings Cross Estate Development is a 67 acre mixed-used business and residential development centred around Kings Cross and St Pancreas rail stations in central London: https://www.kingscross.co.uk/the-story-so-far