JUSTICE COMMITTEE

SCOTTISH BIOMETRICS COMMISSIONER BILL

SUBMISSION FROM SCOTTISH CENTRE FOR CRIME AND JUSTICE RESEARCH (SCCJR), UNIVERSITY OF STIRLING

I support the overall principles of this Bill proposing the establishment of a Scottish Biometrics Commissioner. Relevant points and questions for consideration include:

- An ethics advisory group should be established to work with the Commissioner – as recommended by the Independent Advisory Group on the Use of Biometric Data in Scotland (2018), and as is the case in England and Wales.
- Give further consideration as to whether or not the remit and scope of a Scottish Biometrics Commissioner should be extended to include other authorities involved in criminal justice and community safety, beyond that of Police Scotland and the SPA. For example, consider whether the Scottish Prison Service needs to be included.
- If electronic monitoring technologies are introduced in Scotland which involve biometric data, then it is worth considering whether the relevant bodies should be included within the scope of the Scottish Biometrics Commissioner, in the Bill or added in the future.

Question 1: What are your views on the establishment of a Scottish Biometrics Commissioner as a new body to scrutinise the Police?

I support the overall principles of this Bill proposing the establishment of a Scottish Biometrics Commissioner. There is a clear and important need for a Biometrics Commissioner in Scotland. In particular, I welcome the prospect of independent oversight of Police Scotland and the SPA biometric data practices to ensure they are lawful, effective and ethical. I strongly support Section 2(5)a and 2(5)b about the Commissioner having regard for the interests of children and young persons and vulnerable persons. It may be worth considering whether the Commissioner should also have regard for persons with other protected characteristics? In Section 8(1), I advocate adding the Mental Welfare Commission for Scotland and the Care Inspectorate to the list of those the Commissioner must consult on a draft code of practice.

This proposal of increased independent oversight is timely and salient given the rate at which technology is being developed and the uptake by authorities in different jurisdictions. Recent independent academic research by the Human Rights, Big Data and Technology project has raised significant concerns about police uses of live facial recognition technologies and biometric data in England and Wales, raising issues of governance, oversight, privacy and human rights. The research found high levels of inaccuracy in that identity matches were only correct in one fifth of cases, that it may lead to 'surveillance creep' of citizens engaged in routine lawful activities, and that the use of live facial recognition technology had the 'high possibility' of being found to be unlawful (Fussey and Murray, 2019[i]; Booth, 2019[ii]). Rights group Liberty (2019[iii]) have also raised extensive concerns and, in some cases, legal action about police use and private company use of facial recognition technology, emphasising issues of discrimination and inequality in biometric surveillance, criticising its inaccuracy and disproportionate impact on people of colour, young people and women.

I support the awareness raising role of the Commissioner in Section 2(3)b in promoting public awareness, and engaging with concerns about trust, equality, proportionality, privacy and human rights surrounding uses of biometrics in policing and criminal justice. The issues involved go to the heart not only of criminal justice, but of social justice as data is gathered about citizens' lives, affecting how we recognise each other, how we rank or sort each other, how citizens feel about authorities and trust is built or diminished, how decisions are made, how data is shared, and how power and control are used or misused (Susskind, 2018[iv]).

However, in responding to question 2 (below), I want to encourage further consideration by questioning whether a Scottish Biometrics Commissioner should only scrutinise Police (i.e., the wording of question 1) or whether or not their remit and scope should be extended to other authorities involved in criminal justice and community safety, by adding them in the Bill or using provisions to add them in the future.

<u>Question 2:</u> What are your views on the proposed role, responsibilities and enforcement powers of the Scottish Biometrics Commissioner?

The policy memorandum for the Bill repeatedly emphasises policing, forensics and criminal justice, yet it predominantly uses those terms to exclusively mean policing and forensics, not *other* criminal justice bodies and activities which deal with people who have committed crime or are at risk of committing crime, and public protection and community safety activities. People suspected or convicted of crime are rights-holders, too, even in circumstances where some of those rights are lawfully constrained. There are good pragmatic reasons for Police Scotland and the SPA being the highest priority in terms of which bodies are encompassed within the remit of the Commissioner. However, significant use of biometrics occurs in criminal justice beyond that of policing and forensics, and this may expand in the future.

Consider which criminal justice authorities should be within the Commissioner's remit

Examples of biometric data being used in criminal justice systems in other jurisdictions as well as current uses in criminal justice in Scotland are raised here to inform consideration and discussions of the Bill, even if primarily for thinking about future proofing the Bill and deliberating the scope and remit of the Commissioner and the code of practice.

Electronic Monitoring and Reporting in Probation, Parole and Community Justice

Electronic monitoring (EM) technologies which involve biometric data have already been used in probation, prison and parole in countries such as Sweden, Denmark, Spain, Estonia and the United States. These technologies and services monitor people on community orders or release on licence from prison using devices such as smart phones and mobile apps, (body-worn) tags, monitoring units ('boxes' or 'base' units), usually in cases of home detention curfew, and cloud-based software. Some of these electronic monitoring devices can collect different types of data, including biometric data: fingerprint scanning for identity verification; voice identification; text, voice and video communications; facial recognition or iris recognition; location tracking and mapping using GPS, cellular networks and/or Wi-Fi networks; radio frequency monitoring; and portable or remote alcohol monitoring involving a breath-test combined with facial recognition, iris recognition and/or taking a photo to verify remotely if it is the monitored person giving the breath sample. Monitoring of alcohol and drug use encompasses not only justice issues but health issues. Our research shows there are mixed feelings among justice professionals about alcohol monitoring, along with a desire to proceed carefully and collaboratively with any future introduction of alcohol or drug-related EM in Scotland (McIvor and Graham, 2016[v]). Electronic monitoring can be used 'wisely and well' for 'civilised and constructive' and proportionate purposes, or it can be used for punitive and risk-averse purposes in criminal justice (Nellis and Vanhaelemeesch, 2012: 1).

Different from portable monitoring technologies such as tags and smartphones, biometric kiosks have been used in probation and parole, courts and policing in the United States since 1995, and in probation in England and Wales more recently, piloted around 2012, as well as Australia (Raho, 2014[vi]; Nellis, 2017[vii]). Biometric kiosks are a stand-alone electronic machine that look similar to a cash machine, usually installed in criminal justice agency offices. These kiosks enable people with convictions, usually serving a community-based sentence, to come into a justice office and 'check-in' by logging on and reporting through the kiosk, without seeing a criminal justice professional. Biometric data (usually fingerprint or hand scanning) verifies the identity of the individual at the point of logging on. Once identified,

> 'the system will prompt [them] to provide answers to several questions that would typically be asked by a probation officer during a face-to-face visit… including housing and employment status and recent criminal justice involvement (e.g., arrests). Many kiosks also permit probationers to pay fees and fines by depositing funds into a secure lock box attached to the kiosk machine. After the probationer has answered the required questions, the kiosk can be programmed to issue a receipt for a visit and notification to report for a drug test or visit with a probation officer when the probationer's response requires follow-up.' (Ahlin et al., 2016: 690[viii])

Research evidence on the effectiveness of using biometric kiosks is scant (Ahlin et al., 2016). In England and Wales, the 'convenience' and workload and cost-cutting premise behind biometric kiosks attracted strong criticism from the probation union, NAPO, and reform groups such as the Prison Reform Trust (Doward, 2012[ix]).

Fitzgibbon and Lea (2014[x]) contextualise the introduction of kiosks as occurring at a time when probation and community justice in England and Wales was to undergo significant change and semi-privatisation, with services facing pressures to make time and money efficiencies by increasing use of digital services over face-to-face time with staff, and against a backdrop of preoccupation with risk and security in offender management. Failure to report to a kiosk or to provide factual information to a kiosk may potentially be seen as a form of non-compliance with the requirements of a statutory order, requiring follow-up action. The use of biometric kiosks in England and Wales, Australia and the US are mentioned as an example for consideration regarding future-proofing, but kiosks are certainly not being advocated here as something that criminal justice social work and local authorities should consider adopting.

As implied earlier, an emerging area of exploration is how electronic reporting and monitoring can be done remotely using smartphones and apps with biometric verification (without having to come in to a justice office to use a kiosk). Various countries are in the process of developing probation apps and digital platforms, which may have the potential for combination and integration with other forms of electronic monitoring and offender supervision (Graham, 2018a[xi], 2018b[xii]). In research spanning electronic monitoring and digital technologies used in justice work and 'offender' supervision, issues such as proportionality, human rights and privacy, confidentiality, risk and information sharing are raised as priority concerns by criminal justice professionals (Graham and McIvor, 2015[xiii]; McIvor and Graham, 2016[xiv]; Phillips, 2017[xv]; Nellis, 2019[xvi]; Ahlin et al., 2016). For people with convictions expected to carry, wear or use technologies involving biometrics, their views and experiences are important and need in-depth consideration and research because these things can affect trust, mental health, perceptions of legitimacy and procedural justice, (non)compliance and risk of re-offending.

These international developments in electronic monitoring and reporting technologies are worth considering in Scotland in the context of (a) the Management of Offenders (Scotland) Act 2019 and the extent of legislative harmony with this Bill; (b) current and future Scottish Government procurement and uses of electronic monitoring and reporting technologies and services from private companies, and (c) the Scottish Biometrics Commissioner Bill. If electronic monitoring or reporting technologies are introduced in Scotland which involve biometrics, then it is worth considering whether the relevant bodies should be included within the scope of the Scottish Biometrics Commissioner, in the Bill or added in the future.

Prisons

In countries such as England and Wales, Singapore and the United States, alongside traditional biometrics such as CCTV or custody photos, new biometric technologies are being used in prisons, including fingerprint scanners, body worn cameras, video analytics, iris scanners, facial recognition and sentiment analysis (see Burt, 2019[xvii]). In 2019, Her Majesty's Prison and Probation Service (HMPPS) are piloting facial recognition software to verify the identity of visitors, with real time sharing of visitors' faces and data able to be accessed across the prison estate (Mayhew, 2018[xviii]). Given privacy and human rights concerns about prisoners' families and security concerns about visitors bringing in drugs and other contraband, legitimate questions about the use of this data arise. Another example is that of a Spanish company and an American company working together on integrating uses of monitoring technology in prisons as a ‘smart jail eco-system’, including facial recognition and biometric kiosks for day-today use, and ‘liveness detection technology’ with ‘LifeSensors’ monitoring prisoners' heartbeats, respiration (breathing) and agitation levels with the rationale given of suicide risk and detecting heart conditions (Mayhew, 2019[xix]). In effect, some of these biometric technologies are being developed for use with vulnerable people in prison and members of the public who are not prisoners themselves (i.e., families).

Biometrics are currently collected and used with people on remand, sentenced prisoners, and people visiting and working in Scottish Prisons, with some differences between public prisons and private prisons. According to a Freedom of Information (FOI) response by the Scottish Prison Service in August 2019[xx], quoted directly here for the sake of accuracy:

- For individuals held in custody, in public prisons only biometric data held is a photograph, CCTV footage and body worn cameras. HMP Addiewell hold a single fingerprint in addition to the photograph, CCTV and Body Worn Cameras. HMP Kilmarnock hold a single fingerprint in addition to the photograph and CCTV.
- For individuals visiting or working in prisons, public prisons only biometric data held is a photograph and CCTV footage. HMP Addiewell hold a single fingerprint in addition to the photograph and CCTV. HMP Kilmarnock hold a single fingerprint in addition to the photograph and CCTV.
- Information provided to support ongoing Police investigations may be used as evidentiary productions for court purposes.
- CCTV footage may be used for internal adjudication purposes. CCTV will be used to evidence any inappropriate or criminal behaviour within a visit room, which will be used for investigation/prosecution or for the purpose of banning a visitor. HMP Addiewell and HMP Kilmarnock may use fingerprinting to identify a banned visitor, thereby preventing unauthorised entry into the establishment. Photographs are used to identify individuals.
- All the public prisons and HMP Addiewell utilise body worn cameras or hand held camcorders for the purpose of recording planned removals under Rule 91 of the Prisons and Young Offender (Scotland) Rules 2011.
- All Scottish prison establishments utilise CCTV footage for the following purposes:
    - Evidence in any disciplinary proceedings relating to alleged breached of discipline within a prison;
    - Assist SPS in any investigation of an alleged crime; ○ Monitor the movement of individuals throughout a prison; ○ Monitor the movement of vehicles aiding secure entry and exit; ○ Monitor premises deterring and reducing vandalism and other offences; and ○ Recognise people for entry and exit through specific points ensuring only authorised personnel gain access, preventing an escape and unauthorised movement.

Data collected in prisons may be considered to be collected without informed consent, or with limitations on the extent of informed consent.

Biometric data and issues surrounding data collection, use, retention or destruction can come to the fore of public attention in circumstances of deaths in legal custody, police investigation and any subsequent Fatal Accident Inquiries (FAIs), often occurring years later, to establish the circumstances of a death. In FAI reports, Sheriffs have commented on the need for data collection or on preventing data destruction in prisons. There is a Police Scotland standard operating procedure specifically for deaths and serious injury in *police* custody, but in the more general Police Scotland standard operating procedure for investigation of death (see Police Scotland, 2018[xxi]), which lists types of deaths and relevant processes and considerations, there appears to be no section on deaths in *prison* custody. It may be worth checking whether this Bill, as it is currently framed, may or may not incidentally result in any differentiation or bifurcation of oversight of biometrics relating to dying and dead bodies in police custody compared to prison custody? Deaths in legal custody (including prisons) are designated as ‘police reportable deaths’, so the question here relates to whether the Commissioner’s oversight and remit should also include the Scottish Prison Service or whether there is no need as the inclusion of Police Scotland and the SPA is sufficient enough to have oversight of these types of cases.

Local Authorities, Public Surveillance and Community Safety

The Glasgow City Council public surveillance system has the capacity to combine the use of 70 CCTV cameras with recognition software called ‘Person Search’ (formerly known as ‘Suspect Search’). It has been estimated to cost £1.2 million, as part of a £12.6 million upgrade to public space CCTV in Glasgow (Briggs, 2016). According to a Freedom of Information (FOI) response by Glasgow City Council in August 2019[xxii], quoted verbatim here:

- Currently the system can only be accessed by CCTV management from within Glasgow City Council, Neighbourhoods and Sustainability (NS) section and at present this is limited to the Operations Manager for the Glasgow Operations Centre. There are still ongoing operational discussions on the use of the system when it goes live and it is envisaged that access will initially be provided to a restricted staff group from Public Space CCTV operations and Police Scotland CCTV liaison Officers. The only two organisations that will have access to the system will be Glasgow City Council and Police Scotland.

- As part of an upgrade of the Public Safety CCTV (PSCCTV) infrastructure, certain video analytic products have been purchased. This includes Standard Video Analytics (for example detection of perimeter breach) and Person Search which is a sophisticated search engine which can use general descriptions of a person (CCTV image) to aid an operator when searching for individuals. The search would be based on full body image, textures and colours with any unique characteristics, such as colour of clothing, type of clothing (hat/bag), to search recorded CCTV footage for a possible match.

- Person Search is a high-level Video Analytic which will allow community safety staff with authorisation to trace missing individuals, vulnerable persons, individuals involved in crime or antisocial behaviour via a quick launch search engine. The search engine utilises images or descriptions (including CCTV images) to allow the search engine to provide possible matches (thumbnail results) and route information of the individuals concerned. Some of the key community safety benefits will allow operators to help locate or identify missing adults, children or vulnerable people within a shorter timeframe by using the process of image matching based on descriptions provided by already captured CCTV images which would be the reference image upon which the search would be based. The system can also create an avatar based on a description provided if no CCTV image is available, this is generally the case with vulnerable adults who have become separated from their carer or for missing children. It is envisaged that the software will help reduce search times for staff using the system significantly. It does not use facial recognition or emotional recognition and is not linked to any police intelligence databases.
- The data protection impact assessment (DPIA) for Person Search is currently being finalised by Glasgow City Council and will be completed prior to the system going live. Once this is approved it will be published on the council's website.
- Person Search has not yet gone operationally live in Glasgow therefore no evaluation of the system has been undertaken.

Critics (including the Scottish Trades Union Congress) have raised human rights and civil liberties concerns about this software and its use with public space CCTV, and have called for more regulation and independent oversight of local authorities (Briggs, 2016[xxiii], 2019[xxiv]).

The 2016 report by HM Inspector of Constabulary Scotland (HMICS, 2016: 20[xxv]) stated that a Scottish Biometrics Commissioner could 'build capacity and resilience within Scotland to explore emerging human rights and ethical considerations around the use of biometric data by other public agencies including matters which have recently been at the fore of public debate such as biometric data held on public space CCTV systems.' I concur with HMICS on this and encourage Members to consider it further in discussions of this Bill and its scope.

Question 5: Do you have any other comments?

Section 2(4)a of the Bill says 'the Commissioner may, in particular, carry out, commission or support any research it considers appropriate.' Different types of research in this rapidly growing area would be welcome and encouraged in Scotland, especially in building knowledge and awareness; this needs to be strategically planned and sufficiently resourced.

Consider the need for an ethics advisory group to work with the Commissioner
The report and recommendations of the Independent Advisory Group on the Use of Biometric Data in Scotland (the IAG) (2018) are commendable and very relevant to

Parliamentary consideration of this Bill. Recommendation 9 by the IAG (2018: 14) states: ‘An ethics advisory group should be established as part of the oversight arrangements. This should work with the Commissioner and others to promote ethical considerations in the acquisition, retention, use and disposal of biometric technologies and biometric data.’ In its response to this report, the Scottish Government committed to setting up an ethics advisory group. More recently, the Cabinet Secretary for Justice announced a plan to also set up an independent Emerging Technology Group (13 June 2019, to the Justice Sub-Committee on Policing) looking at legal and ethical issues. How the remits of these two groups will be demarcated is of interest.

In England and Wales, there is a Biometrics and Forensics Ethics Group (BFEG). In recent years, their work programme has included looking at, for example, the use of next generation sequencing technologies, international exchange of DNA, ethical principles for stakeholders, retention and use of custody images, DNA paternity testing for child maintenance cases, uses of large data sets by the UK Home Office, and ethical issues and principles to guide police on uses of live facial recognition trials (Biometrics and Forensics Ethics Group, 2019[xxvi]).

Despite multiple references to the complexity and centrality of ethics, the Scottish Biometrics Commissioner Bill and associated memoranda appear to make no direct mention of an ethics advisory group being established to work with the Commissioner. I recognise that this may be because it would not be a statutory group, and there may be a general power for it through section 3(j) and section 8(1)m of the Bill. Nonetheless, I wish to emphasise the need for this group to be established, and I encourage further consideration of it, including provisions of appropriate resources for it to operate and for it to be established in time to work with the Commissioner on a code of practice, alongside other relevant individuals and bodies.

These views are offered from the perspective of a criminologist who researches punishment, criminal justice, justice innovation and technology – not as a professional with qualifications and specific research expertise in ICT, law, policing and forensic science. Members seeking clarification about this evidence submission are welcome to contact me.

Dr Hannah Graham, Senior Lecturer in Criminology, Scottish Centre for Crime and Justice Research (SCCJR), University of Stirling.

[i] Fussey, P., and Murray, D. (2019) *Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology*, Essex: University of Essex. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/LondonMet-Police-Trial-of-Facial-Recognition-Tech-Report.pdf [ii] Booth, R. (2019) ‘Police face calls to end use of facial recognition software’ 3 July 2019, *Guardian.* https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facialrecognition-software?utm_term=Autofeed&CMP=twt_gu&utm_medium=&utm_source=Twitter#Echobox=1562177774

[iii] Liberty (2019) 'Resist Facial Recognition Technology' https://www.libertyhumanrights.org.uk/resistfacial-recognition

[iv] Susskind, J. (2018) *Future Politics: Living Together in a World Transformed by Tech,* Oxford: Oxford University Press.

[v] McIvor, G., and Graham, H. (2016) *Electronic Monitoring in Scotland,* Stirling: University of Stirling.

[vi] Raho, D. (2014) 'The Curious Case of the Use of Reporting Kiosks in the UK Probation Service – Robohero or Roboflob?' Paper presented at the 6th Bi-Annual Surveillance and Society conference, Barcelona 24th -26th April 2014.

[vii] Nellis, M. (2017) *Shaping the Future of Electronic Monitoring in England and Wales – Probation Institute Briefing Paper 1/17,* London: Probation Institute.

[viii] Ahlin, E., Hagen, C., Harmon, M., & Crosse, S. (2016) 'Kiosk reporting among probationers in the United States' *The Prison Journal* 96(5): 688-708.

[ix] Doward, J. (2012) 'Probation officers to be replaced by electronic kiosks in pilot scheme' https://www.theguardian.com/society/2012/apr/28/probation-officers-electronic-kiosksscheme?CMP=twt_gu

[x] Fitzgibbon, W., and Lea, J. (2014) 'Defending probation: Beyond privatisation and security' *European Journal of Probation* 6(1): 24–41.

[xi] Graham, H. (2018a) 'Apps, tags, tracks: Ten questions about uses of technology in probation' Confederation of European Probation https://www.cep-probation.org/apps-tags-tracks-ten-questionsabout-uses-of-technology-in-probation/

[xii] Graham, H.(2018b) 'Using technology in Probation: Reflections on the evidence and questions for Probation work,' Confederation of European Probation Technology Expert Group meeting, Helsinki, 34 September 2018. https://www.cep-probation.org/wp-content/uploads/2018/10/Hannah-GrahamHelsinki.pdf

[xiii] Graham, H., and McIvor, G. (2015) *Scottish and International Review of the Uses of Electronic Monitoring,* Stirling: Scottish Centre for Crime and Justice Research, University of Stirling.

[xiv] McIvor, G., and Graham, H. (2016) *Electronic Monitoring in Scotland,* Stirling: University of Stirling. [xv] Phillips, J. (2017) 'Probation Practice in the Information Age' *Probation Journal* 64(3): 209-225.

[xvi] Nellis, M. (2019) 'Clean and Dirty Electronic Monitoring' Justice Trends https://justicetrends.press/shaping-lives-the-use-of-electronic-monitoring/ [xvii] Burt, C. (2019) 'Singapore prison testing biometrics and video analysis for inmate management' https://www.biometricupdate.com/201902/singapore-prison-testing-biometrics-and-video-analysis-forinmate-management

[xviii] Mayhew, S. (2018) 'Facewatch tech selected for UK prison service facial recognition trial' https://www.biometricupdate.com/201812/facewatch-tech-selected-for-uk-prison-service-facialrecognition-trial [xix] Mayhew, S. (2019) 'Gradiant and Encartele partner on biometric tech solution for the corrections industry' https://www.biometricupdate.com/201902/gradiant-and-encartele-partner-on-biometric-techsolution-for-corrections-industry [xx] Scottish Prison Service Freedom of Information response on 26 August 2019 to an FOI request I made.

[xxi] Police Scotland (2018) Investigation of Death Standard Operating Procedure (SOP) https://www.scotland.police.uk/assets/pdf/151934/184779/investigation-of-death-sop [xxii] Glasgow City Council Freedom of Information response on 16 August 2019 to an FOI request I made.

[xxiii] Briggs, B. (2016) '70 cameras primed for new state-of-the-art surveillance' *The Ferret* https://theferret.scot/70-cameras-primed-for-new-state-of-the-art-surveillance/ [xxiv] Briggs, B. (2019) 'Big brother surveillance could discriminate against workers' *The Ferret* https://theferret.scot/suspect-search-glasgow-surveillance/

[xxv] HM Inspectorate of Constabulary Scotland (2016) *Audit and Assurance Review of the use of the Facial Search Functionality within the UK Police National Database (PND) by Police Scotland* https://assets.documentcloud.org/documents/2702356/HMICS-Audit-and-Assurance-Review-of-theUse-of.pdf

[xxvi] Biometrics and Forensics Ethics Group (2019) *Ethical Issues Arising from Police Use of Live Facial Recognition Technology,* London: Home Office. https://www.gov.uk/government/publications/police-use-of-live-facial-recognition-technology-ethicalissues