JUSTICE COMMITTEE

SCOTTISH BIOMETRICS COMMISSIONER BILL

SUPPLEMENTARY WRITTEN SUBMISSION – KAREN RICHMOND

Thank you for inviting me to provide oral evidence to the Justice Committee on the 24th September 2019. In the course of my evidence I stated that I would provide a supplementary written submission to the Committee on the topic of the Home Office Biometrics Strategy, and the posited solutions to those inter-jurisdictional problems raised in my initial written submission.

Background

This response focusses on issues raised by the Commissioner for the Retention and Use of Biometric Material (CRUBM), Professor Paul Wiles, who was questioned on the problems relating to the use, and retention, of biometric data collected by Police Scotland (and the Scottish Police Authority), and routinely copied to UK databases sited in England. Professor Wiles responded as follows;

> *'I think that the answer…is that, if the biometric samples or biometric profiles in the case of DNA are Scottish, Scots law ought to apply. Technically, there is no reason why that should not be done.*
>
> *There are potential problems simply because the databases on which the biometrics are held at UK level are elderly. They are in the process of being replaced, but there has been a delay in that, so there might be some problems because of that. However, with the new databases, I can see no reason why Scottish samples should not be held according to Scottish legislation and English samples held according to English legislation. That would mean that, if the bill is passed and a commissioner appointed, he or she should become a member of the strategy board that oversees use of national UK databases, just as I am.*

That should deal with that matter—although I can imagine one or two issues, at the moment.'[1]

During the course of my own evidence I was asked to comment on the above oral evidence provided by the CRUBM. My response is provided below;

"Professor Wiles alluded to one or two solutions. First, he stated that new databases are coming in, through which the problem might be resolved. Although I do not know anything about that—I could try to find out and send you a written submission—I hope that the new databases that are to replace the existing ones do not replicate their architecture, as that will not resolve the problem."[2]

I have conducted further research focusing on this issue, have liaised with the Office of the Biometric Commissioner for England and Wales, and have sent a number of queries to the Home Office. The results, and my conclusions, are outlined below.

The Legal Status of Scottish Biometric Data

The status and governance of - and responsibility for – DNA, and fingerprint data, deriving from samples taken in Scotland by either Police Scotland or the Scottish Police Authority, is problematic. At present, copies of DNA profiles, and sets of fingerprints (known as 'tenprints') - collected under Section19C(2)(c) and (d), of the Criminal Procedure (Scotland) Act 1995 - are routinely sent to England for loading onto the National DNA Database (NDNAD), and the National IDENT1 fingerprint database.

These databases fall within the ambit of the CRUBM. However, the Commissioner's statutory powers only extend to biometric samples taken in England and Wales under PACE S.63D(1)(a) and (b) (and a number of counter-terrorism statutes). The CRUBM has stated that, as far as he is

[1] Official Report, Justice Committee of the Scottish Parliament, Tuesday 24 September 2019, at p.3
[2] *Ibid.* at p.18

concerned, if copies of data sent to the national databases by Police Scotland are Scottish in jurisdictional origin, then Scots law ought to apply. While the willingness of the CRUBM to accommodate Scots Law may signal a welcome level of inter-jurisdictional cooperation, this only serves to crystallize the issue.

Absent of a primary legislative amendment to Section 20 of the Protection of Freedoms Act 2012, worded so as to either bring these 'Scottish' samples within the ambit of the CRUBM's powers, or to extend the ambit of the Scottish Biometric Commissioner to both the Ident1 and NDNAD databases, these samples would continue to enter a regulatory lacuna between PACE and the CP(S)A95. In practice, this entails that a citizen of England or Wales whose biometric samples and data are collected under PACE would be afforded certain rights relating to the use and retention of their data on the national databases. Individuals whose samples and data were collected in Scotland would find themselves comparatively disadvantaged, since, in summary, the Scots legislative provisions (and powers of the SBM), extend no further than the Scottish jurisdiction, and the CRUBM enjoys no powers over the retention and use of Scots samples copied to national databases.

The Home Office Biometric Strategy[3]

The CRUBM expressed a further opinion that a solution may be arrived at through the introduction of a new biometric platform by the Home Office. This centralised system will replace the existing IDENT1 and NDNAD databases, with a 'technically converged' platform which will interface with police stations, mobile collection facilities, ports of entry, and visa application centres.[4] It will also retain the flexibility to accomadate new, and developing, forms of biometric data.[5] The Home Office Privacy Impact Statement states, at page 3, that

[3] See The Home Office, *Biometrics Strategy: Better public services, Maintaining public trust* June 2018 (London: The Home Office); https://www.gov.uk/government/publications/home-office-biometrics-strategy
[4] *Ibid.* at page 7
[5] The Home Office, *Home Office Biometrics Programme Privacy Impact Assessment* 2nd May 2018, (London: The Home Office), at page 11. Strategic Facial Matching for Law Enforcement

'The HOB Programme will transform the existing siloed biometrics capabilities into a technically converged, but commercially disaggregated, strategic biometrics capability.'[6]

In terms of architecture, the 'biometric platform - referred to as the HOB "Biometric Services Platform" (BSP) - comprises 'front-end' equipment (with mobile interfaces), which will be located in a number of distributed sites, most notably police stations, and will provide the enrolment and data capture capabilities. The BSP also consists of the 'back-end' Biometric Services Core, which includes the main service-providing subsystems such as the Biometric Services Gateway (BSG), Central, Bureau, and Matcher sub-systems. For the purposes of the present discussion, it is this HOB central platform which is of interest, as this contains all biometric data located in one physical space.

Technical Centralisation and Role-Based Access

The Home Office Privacy Impact Statement posits that 'while all the collections of data will be physically within one system they will however be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access.'[7] This is a source of concern for the CRUBM, who states in his 2018-19 Annual Report, at paragraph 46,

'There is nothing inherently wrong with hosting a number of databases on a common data platform with logical separation to control and audit access but unless the governance rules underlying these separations are developed soon then there are clear risks of abuse. This risk has already crystallised.'[8]

The CRUBM proceeds to cite an example in which the Ministry of Defence gained access to a number of discrete databases, no clear access protocol

---

was accepted into the HOB scope in March 2017. The project will deliver a new algorithm with storage and retrieval for law enforcement facial image matching,

[6] *Ibid,* at page 39, Annex E. No agencies or institutions in Scotland were consulted.

[7] *Ibid.* at page 5, Paragraph 1.3

[8] Commissioner for the Retention and Use of Biometric Material, *Annual Report 2018-19*, (Office of the Biometrics Commissioner: London)

having been in place. Further, the CRUBM highlights a lack of clarity, assurance, and oversight.

> 'What does not seem to have happened…was to establish clear access rules to the different databases held on… a multi-user data platform. [The above example] illustrates why I regard it as urgent that access rules and appropriate governance arrangements are decided upon and implemented before the new HOB data platforms come into use.'[9]

A greater onus is placed on SPA and Police Scotland (and consequently on the SBM), to ensure stable and lawful access protocols to any National databases to which Scottish samples are uploaded, since these authorities *voluntarily* provide copies of biometric samples and data to the UK databases, rather than doing so in compliance with legislative requirements.

The addition of new forms of biometric data to these national databases may engender deeper problems, traceable to this lack of physical, or administrative, disaggregation. Notably, the supporting Home Office BSP documentation gives frequent indications of the ways in which they envisage the platform being used, and evolving. The continued use of the term 'siloed' to refer to exisiting arrangements is notable, since 'siloing' properly refers to the phenomenon whereby particular centres of organization and activity become isolated in terms of their constituent processes and systems. This occurs when domains, departments, or management groups, do not share information, goals, tools, priorities and processes with other departments. Or it may occur when the networks which facilitate the sharing of goals, are attenuated or unavailable. The use of such a terms to refer to necessary disaggregation and restriction with respect to biometric data is a cause for concern.

[9] *Op cit.*

Conclusions

Taking the above into account, the optimal legal solution - which would ensure that the Scottish Biometric Commissioner has proper oversight of all biometric samples collected in Scotland, and copied to UK databases - would be for both the original samples, and copied data, to remain in Scotland. Given that the tendering process, and implementation of the new Home Office Biometric platform, has been delayed, it may yet be possible to request that the database be both logically - *and physically* - disaggregated, such that samples collected by SPA (or Police Scotland) remain on a jurisdictionally separate platform, located in Scotland, albeit that this discrete platform forms an accessible component of the larger Home Office Biometric platform.

It is conceivable that this is the course of action that the CRUBM envisaged, when he referred to the hosting of samples under two legal jurisdictions. This process would be further facilitated through the SBM joining the HOB strategy board, a measure which was, again, recommended by the CRUBM. Such measures would align with the ambitious nature of the Scottish Biometric Commissioner Bill, whilst providing a stable and coherent legal platform for the development, and accommodation, of future forms of biometric data.

Karen Richmond