Rt Hon Greg Clark MP, Chair
Science and Technology Committee
House of Commons
(By e-mail)

OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

24 June 2021

Dear Chair

Previous Committee Report, Work of the Biometrics Commissioner and the Forensic Science Regulator

Having seen your letter to ministers dated 5 May 2021 and in advance of the next scheduled meeting of your Committee listed for 30 June 2021, I thought it might be helpful if I set out some brief observations relating to the subject matter under consideration so far as it is affected by my roles.

Since taking up responsibility for the statutory roles of the Biometrics Commissioner and Surveillance Camera Commissioner in March of this year I have received a good deal of correspondence, but the mailbox has been dominated by only 3 letters: A.F.R. That a single technological application such as Automated Facial Recognition can foreshadow every interview, presentation and conversation is, on the one hand, perhaps indicative of how narrow the debate is becoming while, on the other, possibly a proxy measure for stakeholder concern around the introduction of innovative technology in biometrics and surveillance more generally. Either way it underscores the importance and exigency of the challenges ahead.

I have come across many examples of police surveillance systems that have been roundly discredited in various jurisdictions and it is probably true that their use has eroded public trust, perhaps because they were not appropriately validated in advance, perhaps because they jumped the gun and almost certainly because they were not properly explained, consulted upon and deployed under clearly defined policies. It is my firm belief that people must be able to have confidence in the *whole ecosystem* that uses surveillance and biometrics, now and in the future. This belief very much mirrors the Committee's observations that the development and use of biometric technologies must "involve as much public awareness and engagement as possible, to ensure that there is public trust" in them[1]. To that end the Committee may be interested to note the following areas of activity that I have undertaken since March:

Regulation, standards and governance

1. All local authorities and police forces are under a clear legal duty to have regard to the Surveillance Camera Code when operating surveillance camera systems[2]. The Home Office has revised the Code and a draft is ready for consultation on a date to be announced by ministers. I have contributed to the draft and am confident that the revised Code will, subject to the will of Parliament, take account of the relevant elements of the Court of Appeal judgment in *Bridges v Chief Constable of South Wales* Police[3]. A further practical example of where the Code might improve standards and regulation in one of the fastest-growing areas of public concern in the surveillance of public space is in the use of drones. The revised

[1] Committee Report, session 2017-19, published 18 July 2019: Work of the Biometrics Commissioner and the Forensic Science Regulator, para 27.
[2] Protection of Freedoms Act 2012, s. 33(1).
[3] *R (on the application of Bridges) v Chief Constable of South Wales Police & Ors* [2020] EWCA Civ 1058.

Code could readily be incorporated by the Civil Aviation Authority (CAA) into the licensing arrangements for drone pilots, inexpensively and immediately, and I have met with industry standards bodies and insurers and have made a joint approach to the CAA.

2. Following the May elections, local police and crime commissioners must now publish their statutory police and crime plans under the relevant legislation. As the democratically accountable representatives of their communities these PCCs/PFCCs/Deputy Mayors for Policing and Crime are responsible for understanding their communities' awareness of, and support for/opposition to the use of biometrics and surveillance technology by the police and for holding their chief officers to account for its procurement/deployment accordingly. I have met (virtually) with Alun Michael (PCC for South Wales) to see how we might work together to reinforce the impact that local democratic accountability can have in relation to public awareness and engagement and to achieve balance in the public debate which sometimes appears to presume a general opposition to the use of new technology by the police in this area (a presumption that is not necessarily borne out in the research). I have also begun discussions with police areas about how my office can assist in the drafting of relevant police and crime plans in this regard.

3. With the new Forensic Science Regulator now place to take forward the measures under the 2021 Act, Gary Pugh and I have already met to consider how we can co-ordinate standards and regulation activity to ensure that the advances in technological capability are matched by a corresponding increase in transparency, legitimacy and trust.

4. The Committee has previously commended the approach to biometrics regulation being adopted in Scotland. I have met (virtually) several times with Dr Brian Plastow, the new Scottish Biometrics Commissioner, and have been appointed to his Advisory Group in order to share best practice and endeavour to achieve a coherent approach across our respective jurisdictions. I am also a statutory consultee under the Scottish legislation.

5. Comparison of the emerging approaches in other jurisdictions has also led to my taking part in a number of events to discuss proposed *moratoria* or even outright proscription in relation to the police use of technology. While these are properly and entirely matters of policy for the relevant jurisdiction, they engage a broad principle of police accountability that is applicable here. Whether the police decide to use a tactical option in any given case is a fundamental part of their operational discretion and they will be as accountable for a decision *not to use* technology as they are for using it. To deny them access to available tactical options, it seems to me, not only encroaches on their operational independence but also *dilutes* their accountability.

Retention of custody images and biometric material

6. I have noted the Committee's ongoing concerns around the retention of custody images of unconvicted individuals. As the pandemic measures have been relaxed I have been able to restart the programme of police force visits to scrutinise the retention and use issues within biometrics and surveillance camera systems and, while it is not one of my express functions, I have included an element to ask police forces how they are notifying people of their entitlement to have their images deleted in the event of their being 'No Further Actioned' and to what effect; I will also be asking what measures are in place locally for the manual deletion

of such images and to mitigate the risk of these images being used when compiling 'watchlists'. Interestingly, since taking up my role I have met many people who believe that the police use of automated decision-making in facial databases should be outlawed. As the Committee has noted, any effective deletion of custody images relies on automated decision-making, providing a small example of how technical complexity and public trust may pull in different directions simultaneously in this area (and how outright bans can produce unintended consequences).

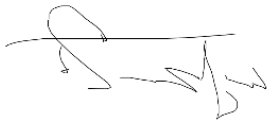
7. In his Annual Report in 2019 my predecessor for biometrics functions reported that almost 300,000 fingerprint records were being held unlawfully as they did not meet the requirements of s18 of the Counter-Terrorism Act 2008[4]. The situation remains the same a year on. As with custody images the solution is automated deletion software and the Home Office Biometrics Programme have outlined their plan to develop an automated deletion tool, however progress appears to be rather slow. I have visited Counter-Terrorism Policing on several occasions and have noted that they have dedicated resources to conduct 'business as usual' deletions to prevent the volume creeping up and ensured that their the unlawful holdings are held in an unsearchable format.

Conclusion

The issues above comprise a combination of risks and challenges arising from the introduction of new technological capability and those that are a legacy from a previous era. If we are to achieve greater public trust in the introduction of new technology in the area of biometrics and surveillance any framework of standards, regulation and governance must be consistent, coherent and comprehensive, giving appropriate attention to both. In this regard I believe it is important to recognise retention - of biometric material, images and other forms of data - as being the product of a deliberate and purposive decision rather than a 'default' position of non-deletion and I included this in my response to the statutory consultation on the new guidance to replace the Management of Police Information (MOPI)[5].

In its analysis of the wider challenges raised by facial recognition technology in policing[6] the Bennett Institute for Public Policy advocates for a "layered, co-governance approach". As the new incumbent of one such layer I look forward to working with the Committee and the many other stakeholders in co-governance to ensure that we proceed in a way that balances technological capability, legal permissibility and societal acceptability.

Yours sincerely



Professor Fraser Sampson,
Biometrics and Surveillance Camera Commissioner

---

[4] Section 18 of the Counter-Terrorism Act 2008 requires that, where biometric material is received from foreign law enforcement bodies or other UK agencies, it may be retained in the first instance for three years but thereafter only if it either has been received without any biographical identifiers or has been made the subject of a National Security Determination.

[5] https://www.college.police.uk/article/information-records-management-consultation accessed 24 June 2021.

[6] *Governing Live Automated Facial Recognition Systems for Policing in England and Wales*, Duan, F.I., December 2020, University of Cambridge.