OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

The Data Protection and Digital Information (No. 2) Bill Committee

By email

15 May 2023

Dear Committee Members,

Data Protection and Digital Information (No.2) Bill: oversight of biometric data

I write with regard to clauses 104 and 105. The former abolishes the office of Commissioner for the Retention and Use of Biometrics and the latter repeals both the duty on the government to publish a Surveillance Camera Code of Practice governing the use of public space surveillance systems by police and local authorities and the requirement for a Surveillance Camera Commissioner to oversee it.

As the officeholder expressly appointed to cover the functions of both commissioners I am responsible for keeping under review the retention and use by the police of DNA samples, DNA profiles, and fingerprints; deciding applications by the police to retain DNA profiles and fingerprints; reviewing national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints; encouraging compliance with the Surveillance Camera Code; reviewing how the code is working; providing advice to ministers on whether the code needs amending and providing reports to the Home Secretary about the carrying out of all my functions.

I responded to the DCMS consultation, 'Data: a new direction', on 2 November 2021[1]. While not rehearsing the points raised there, I would respectfully direct the Committee's attention, in particular, to 5.7, 7, and 9 of that response concerning my non-regulatory functions, non-data protection issues, and issues about 'absorption' or alternatives to the current

[1] https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version

arrangements. Moreover, the policy behind these clauses is that public space surveillance technology by the police is simply a matter of data protection and will be sufficiently regulated under the UK's wider data protection regime without the need for additional commissioners. As indicated in my consultation response (10.5.3-10.5.5), this raises a devolution issue for Scotland which has its own Biometrics Commissioner with whom I work closely. Data protection being a reserved matter, the Bill will put the use of cameras (roadside, body worn or facial recognition) by Police Scotland beyond the Scottish Biometric Commissioner's purview now and in the future. Further considerations affecting Northern Ireland are also identified in my response (10.6.1-10.6.3).

By way of a single illustration of my work which, under the Bill's provisions, would fall neither to the Investigatory Powers Commissioner nor to the new Information Commission it proposes to create, I would cite the procurement and use of Chinese surveillance technology.

On 24 November 2022 the Chancellor of the Duchy of Lancaster made a statement in the House of Commons instructing government departments to cease deploying visual surveillance systems onto sensitive sites where they are produced by companies subject to the National Intelligence Law of the People's Republic of China. The statement noted that this instruction followed a review undertaken by the Government Security Group. Behind that decision, and the related decisions of policing and local government bodies - and even commercial retailers – has been a significant amount of work undertaken by my office which I can confidently say has been at the forefront of raising the risks of procuring and using such technology, both nationally and internationally. I believe we have been instrumental in achieving this first step in addressing the use of public surveillance technology with a foreign provenance, a belief corroborated by the acknowledgement from the current Minister for Security and other parliamentarians. The international recognition of, and response to, the ethical and security risks arising from this public space surveillance issue stands as an example of the 'non-data protection' work undertaken by my office that is not addressed within the Bill. There are many other examples including the surveys of police forces and local authorities in their use of surveillance camera technologies, and visits to police facilities to review the retention and use of biometrics and to assist local elected policing bodies hold their forces to account (in relation, for example, to

the unlawful retention of large volumes of foreign law enforcement records, which I discuss in my 2021/2022 annual report[2].

At this stage in the Bill's Parliamentary passage, my principal concern remains: there is no provision for these non-casework biometrics functions and 'non-data protection' issues in relation to public space surveillance. The Bill does not provide for these matters, and I am not aware of any meaningful plan to address them once the statutory offices are abolished. How the proleptic Information Commission will operate cannot be known until it is established by the Bill but some certainty might be ensured within the detail of the Commission's express statutory functions. And while the Home Office have suggested informally that there are other statutory bodies with the potential to absorb some of this work (for example the Equality and Human Rights Commission) it is difficult to see how they can be expected to express a considered view on their preparedness to absorb responsibilities which are not even broadly described anywhere. Finally, it is worth noting that police accountability in their use of new technology such as facial recognition, voice pattern analysis and other AI-driven capabilities is one of the most contentious aspects of biometric surveillance yet remains unaddressed, either in the Bill (the focus of which remains solely the regulation of DNA and fingerprints in certain, limited circumstances) or at all. As an advocate of the accountable and proportionate use of new technology by the police I think this lacuna is problematic as much for the police themselves as for the communities they serve.

To help understand the relative importance of these functions and address the risks (whether in statutory provision or otherwise) I have commissioned an independent gap analysis by two leading academics, Professors Pete Fussey and William Webster, who have extensive experience and recognised expertise in the information, surveillance and privacy arena and who appear to me to be well placed to provide an objective, evidence-based commentary for the benefit of those tasked with policymaking and the individuals who come after me once my office has gone.

The gap analysis remains incomplete, but the interim findings suggest that there may be significant gaps were the Bill to proceed in its current form. I attach that interim report as an annex to this submission.

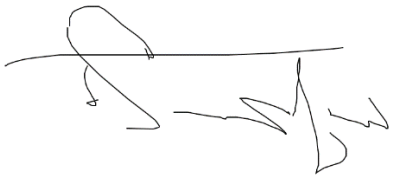
---

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Having agreed to be reappointed while the Bill progresses through Parliament, I am grateful for the Committee's attention in this matter and am willing to provide any other information or explanation that might be of assistance.

Yours sincerely



Professor Fraser Sampson
Biometrics and Surveillance Camera Commissioner

OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Annex to the Biometrics and Surveillance Camera Commissioner's submission to the Bill Committee for Data Protection and Digital Information (No.2) Bill: oversight of biometric data.

Interim findings of an independent report on changes to the office of the Biometrics and Surveillance Camera Commissioner (B&SCC) functions arising from the Data Protection and Digital Information Bill.

1. Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. These new and advancing technologies hold clear potential to enhance public safety yet also have the capacity for enormous harms. The possibilities for integrated surveillance technology, driven by AI and supported by the internet, create genuine public anxieties over civic freedoms. These anxieties exist across almost all jurisdictions. Within this context, consideration of genuine, meaningful and trustworthy governance and oversight is urgent and pressing.
2. In current form, the Bill will delete several surveillance oversight activities and mechanisms that are set out in legislation and arise from the fulfilment of statutory duties placed on Commissioners. Prominent among these is the tabled abolition of Protection of Freedoms Act 2012 (POFA) legislative requirements to (a) appoint a Surveillance Camera Commissioner and (b) to publish a Surveillance Camera Code of Practice, which offers governance coverage far beyond data-related issues. The Code is realised through the national Surveillance Camera Strategy, which would also disappear. The value of the Code and Strategy for providing surveillance oversight, raising standards in surveillance practice, delivering guidance for camera users, and offering transparency and public confidence is set out in more detail below.
3. The other functions of the Biometrics and Surveillance Camera Commissioner are manifold and comprise both judicial and non-judicial elements. Key activities and benefits include, but are not limited to developing, and encouraging compliance with the Code; raising standards for surveillance camera developers, suppliers and users; public engagement, and building legitimacy and consent for surveillance practices; annual reporting to Parliament via the Home Secretary; convening expertise to support these functions; reviewing all National Security Determinations and other powers by which the police can retain biometric data.
4. Surveillance oversight is historically and currently overburdened and under-resourced. Activities undertaken by the SCC component have extended the Commissioner's role, not in terms of regulatory overreach, but to compensate for this shortfall, thereby raising standards and increasing professionalism across the sector. While not defined in the original legislation (POFA), these activities

have arisen *as a result of successive Commissioners fulfilling their statutory duties*. The Bill proposes the erasure of many such functions and, by extension, their associated value to society. As one expert interviewee for the report expressed, having been based on a consultation about 'absorption' of the functions by the Information Commissioner "the Bill makes no provision for absorption whatsoever. It just deals with extinction". For example, the Bill contains no provision for continuing the work of driving up standards for the development, procurement, adoption and use of surveillance cameras, a programme of work widely applauded across police, practitioner and industry communities.

5. The value of these activities is widely recognised and easily evidenced across civil society organisations, industry professionals, Parliament, and law enforcement communities. Of the latter, it is important to acknowledge significant evidence of (a) police support for the SCC role and (b) requests for clarity over appropriate uses of surveillance tools.
6. The POFA Commissioners' functions are not regulatory in the same sense as the Information Commissioner (ICO). This difference has several implications. First, the roles are not directly comparable with ICO. Consequently, the impact of SCC functions arises through different and sometimes less visible or direct means. It also means elements cannot be directly "lifted and shifted" into a different regulatory format and destination.
7. Also crucial is that these activities extend significantly beyond matters of data use. Considering surveillance impacts and harms purely in terms of data protection is widely recognised as a highly restrictive and selective framing. It is also widely acknowledged that rights concerns arising from surveillance are not reducible to issues of privacy alone. One could further argue that adding POFA to the existing data protection landscape constituted recognition of this over a decade ago.
8. Advanced digital surveillance, particularly AI-driven forms, is a global phenomenon. The Bill's reduction of surveillance-related considerations to data protection compares unfavourably to regulatory approaches in other jurisdictions. Many have started from data protection and extended to cover other germane issues. Examples include EU proposals around an AI Commissioner, and the MEP vote to support a compromise text for the AI Act that bans public uses of remote biometric identification (including facial recognition) on 11 May 2023.
9. Examples of these wider activities and their impact are:
    a. The BSCC's recent success in addressing widespread use of Chinese cameras with known cyber vulnerabilities in sensitive UK sites. The development of these tools is also associated with significant human rights abuses.

b. Automatic Number Plate Recognition (ANPR) surveillance operates on one of the largest databases in Europe. It has grown from a local to a national network, from focused counterterrorism uses to monitoring urban clean air zones and car park ticketing. Credible estimates suggest a likely 100 million daily ANPR data acquisition points from 2024. ANPR grew with little data protection-related scrutiny. The SCC role brought proactive engagement that established an independent advisory group to provide standards and governance for this technology, and to convene key stakeholders (including the police) into this activity.
c. SCC established current guidance to law enforcement concerning lawful and ethical use of facial recognition. This guidance transcended data protection issues, addressed standards, transparency, ethics, human decision-making and the authorisation of deployments. It is now incorporated into NPCC guidance.

10. The Bill removes reporting obligations currently in POFA Commissioner roles. This removes a mechanism for assuring Parliament and the public of appropriate surveillance use, affecting public trust, and legitimacy invested in surveillance practices. We are at a critical moment concerning public trust in institutions, particularly law enforcement, something central to the success of UK policing. As drafted, the Bill reduces public visibility and accountability of related police activities.
11. The independence of oversight is similarly crucial to public trust. Clause 28 of the Bill requires the new Information Commissioner to respond more explicitly to “strategic priorities” designated by the Secretary of State. This may risk diluting public trust and confidence in the paramount condition of independent oversight.
12. The Bill seeks to transfer some responsibilities outlined in POFA (fingerprints and DNA) to other entities, allow others to lapse, and makes no provision to the functions and oversight activities arising from several POFA Commissioner duties. One argument has been that many SCC activities are not defined in POFA and therefore cannot be transferred. However, the Code enables the SCC to provide and issue guidance across the surveillance landscape. It also requires ‘relevant authorities’ to comply with its principles. These are two powerful requirements which hold state institutions to account yet the Code is to be deleted. Several issues arise from this decision to restrict formal transfer of only those biometric responsibilities specified in POFA and deleting anything relating to surveillance camera standards.
13. Biometric technology is expanding and diversifying at an unprecedented rate. Specifying only those biometric techniques mentioned in legislation of over a decade ago challenges notions that the Bill is “future proofed”. By designating a

part of fingerprints and DNA retention to the Investigatory Powers Commissioner (IPCO) also risks a de facto segregation in the oversight of different biometrics techniques, where the governance of all other forms rests in other as yet unidentified places. It removes any statutory duties from the interface of biometrics and surveillance, the policy basis on which ministers recently combined the POFA Commissioner functions. Moreover, one could argue that given the potential for collateral intrusion, remote biometric surveillance resonates more closely with IPCO's remit than fingerprints and DNA.

14. The original proposal consulted on was for all POFA biometric and overt surveillance functions to be absorbed by the ICO. The Bill reflects the view of many that biometric casework sits more naturally with IPCO. Expert interviewees for the report highlighted how most gaps left by this Bill could also be addressed if responsibility for the Surveillance Camera Code (only recently approved by Parliament) also moved under IPCO. This would harmonise all functions for oversight of traditional and remote biometrics in policing under one established and internationally regarded judicial oversight body. Such a move could also add genuine 'future proofing' by anticipating the increasing potential for blurring boundaries between overt and covert surveillance brought by new advances in technology.
15. Academic research has demonstrated significant public concern over one such form of remote biometric monitoring, facial recognition technology. Other experts and public bodies have called for more detailed rules for uses of this technology in public. A stark contrast exists in the working of the Bill between mention of relatively uncontroversial decades old biometric techniques and the cutting-edge technologies currently animating public debate. Reference to "remote biometric identification" could be one entry point to addressing this issue.
16. This issue is made more pressing given the Policing Minister expressed his desire to embed facial recognition technology in policing and is considering what more the government can do to support the police on this. Such embedding is extremely likely to include exploring integration of this technology with police body worn video (interview with the BSCC).
17. Excluding IPCO, expert interviewees questioned the suitability of alternative venues for surveillance and biometric oversight. This issue invokes several considerations. One concerns thematic coverage and the spectrum of potential surveillance harms that transcend data-related matters. Additionally, two organisations have been highlighted as possible venues for absorbing public surveillance oversight functions: a modified Information Commissioner's Office and, separately the Equality and Human Rights Commission. Taking these in turn, POFA oversight is mostly limited to the activities of public bodies. Existing data protection regulation covers both public and private entities. Housing

oversight in the latter may provide wider scope and address complexities of regulating public-private surveillance activities. However, research has demonstrated the limited role data protection controllers have played in providing enforcement against breaches in relation to video surveillance in a significant number of countries including the UK. In addition, without further specific legislation the EHRC are arguably not currently constituted to legitimately address many of the functions and activities outlined above and the totality of surveillance oversight needs.

18. It is widely accepted that current oversight of complex surveillance practices is considered patchy and requires simplification. Simplifying oversight has been consistently stated as a key aim for the Bill. However, such simplification entails at least three further considerations:
    a. Calls for simplified oversight correctly include a requirement for companion policies for implementation and compliance. These translate abstract principles into clear guidance and standards for users of biometric and other surveillance technologies while offering mechanisms for auditing compliance. This relationship between law and policies was central to the *Bridges* Court of Appeal judgement on facial recognition technology in light of which the Home Secretary amended the Code. The Bill contains no mention of guidance or compliance mechanisms aside from those pertaining to data management. The absence of requirements for guidance and to ensure compliance generates vulnerabilities for users of these technologies and for the rights of individuals subjected to them and is particularly important given the significant uncertainties brought by emerging technologies.
    b. Simplification is an important ambition but should not come at the expense of meaningful oversight. For example, as one expert interviewee remarked, “why is it that simplification is more important than raising standards?”
    c. What may appear a simplification in organisational terms does not naturally translate into a simplification in a practical sense. As stated above regarding different biometric techniques, this ambition for simplification may actually complicate the oversight landscape. Removing a Commissioner who proactively interfaces with developers and users of surveillance technologies may generate future difficulties. For example, it may take longer for aspiring technology users to access knowledge. In addition to impacting public resources, pressing ahead with surveillance deployments before such advice is received may generate greater exposure to litigation for public bodies. Alternatively, the absence of such information may lead users to highly conservative interpretations of the

law which may dissuade legitimate uses of surveillance technology for public safety.

Professor Pete Fussey and Professor William Webster, 11 May 2023