OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

Lucy Allan
Member of Parliament for Telford

[redacted]

12 May 2023

*Letter by email*

Dear Lucy

**Risks from Use of Surveillance Cameras Around MPs' Home Addresses**

I write in response to your email of 8 May 2023 seeking advice on the operation of surveillance cameras around the homes of members of Parliament.

While I should state at the outset that the description of the surveillance camera system to which you refer appears to take it outside my statutory functions, the questions you have raised are frequently – and increasingly - raised with my office; given their relevance to the proliferation of biometric surveillance generally and the future regulation of this area, I thought it appropriate to offer some views which are intended to be helpful.

**Regulatory framework**

As we do not enjoy any freestanding right to privacy as such in the UK, most of what people worry about under this head derives protection from the European Convention on Human Rights, art 8 of which extends a qualified and broader entitlement to private and family life. Plainly that covers some of the areas that you refer to although there are other areas of human rights that are often engaged by intrusive surveillance such as the right to freedom of speech, thought, assembly and so on.

Against that background intrusive surveillance is generally dealt with as a matter for data protection and the framework providing rights for the citizen comes under their interests as 'data subjects'. The Government's formal view is that all overt ? surveillance is really a data protection matter and, as the UK data protection authority is the Information Commissioner, private surveillance concerns fall under his aegis as part of the Data Protection Act 2018 and the General Data Protection Regulation and their principles. The Information Commissioner has provided public guidance on the use of surveillance cameras and there have been some private actions by householders against neighbours deemed to have been improperly using surveillance equipment, although none of these cases has, to my knowledge, been brought in the higher courts and therefore the judgments are not binding on other courts or tribunals.

Under the current regulatory framework, the only legal instrument expressly regulating the standards for installing, operating and reviewing surveillance camera systems and their use is the Government's Surveillance Camera Code of Practice (the Code). Published by the Home Secretary under the Protection of Freedoms Act 2012 the Code sets out specific and detailed obligations and expectations of operators of surveillance camera systems beyond purely data protection considerations reflecting Parliament's view that the use of surveillance cameras in public space required greater regulation than simply the general protection of data subjects. The legal duty to have regard to the Code is limited to the police and local authorities but increasingly commercial businesses are seeing the attractiveness of voluntarily adopting the Code and its principles and one of my functions is to encourage its adoption. The Code was revised by Parliament in February 2022 and can be found here . It is however to be abolished under the Data Protection and Digital Information Bill currently before Parliament.

Clearly the surveillance camera system you describe does not fall within the provisions of the Code.

**Surveillance concerns**

As you identify in your email, the technological reality is that modern surveillance devices are no longer CCTV cameras – or cameras at all - but powerful computers one basic function of which is to capture, store and share images. Most modern surveillance systems (whether they be doorbells, dashcams, body worn devices etc.) are connected or at least capable of being connected to the internet and their 'cameras' have IP addresses. Surveillance systems come with latent functional capabilities allowing, for example, automated number plate readers (ANPR), sound and language monitoring and even facial recognition and it is almost impossible even for the owner/installer to say confidently which functions are running at any given time. Exponential growth in biometric surveillance means that private citizens now have access to technology that was only recently the preserve of state intelligence agencies. Add to this the expansion of Artificial Intelligence (AI), reinforcement learning and generative training in biometric surveillance, advances such deepfake technology, cyber hacking and the ability to synthesise and analyse meta data about individuals and it becomes clear that we are already aeons away from the traditional concept of static, monofunctional, closed-circuit TV cameras with which most of us grew up.

Against that technological background there are ethical and security risks that are relevant to your correspondence.

**Ethical and security risks**

Insofar as the manufacturers and suppliers of the surveillance equipment are concerned, I have made my views on the evidenced ethical and security risks presented by companies such as Hikvision and Dahua known to ministers and to Parliament, most recently to the Joint Committee on Human Rights. The House of Commons Foreign Affairs Committee reached its own damning conclusions in its report of 2021.

While the ethical considerations in expending public money with such companies and deploying their products are properly matters for public scrutiny, private

procurement is of course a matter for the individual. However, the security risks arising from the acquisition, storage and sharing of surveillance data from such equipment are relevant in any setting and particularly so in the case of specific occupations, activities and individuals. Those risks were finally formally acknowledged by the Government last November with ministers ordering government departments to remove Hikvision cameras from 'sensitive sites' on the basis that they represented a significant security risk; other departments and organisations have been encouraged to review their arrangements accordingly and some councils and policing bodies have decided not to use certain surveillance partners in the future. As I have pointed out to ministers and officials, 'sensitivity' can arise in many forms including electoral and other democratic circumstances; your situation and the use of intrusive surveillance capability in and around the private lives of MPs provides a clear example of another. Having been CEO to the Police and Crime Commissioner in West Yorkshire at the time of the appalling murder of Jo Cox MP, I read your email setting out the particular sensitivities and security issues faced by MPs with that dreadful event very much in mind. Given that several leading providers of surveillance technology are no longer trusted by our Government and partnersI continue to question where people can seek and receive assurance in relation to the risks of who is operating and accessing surveillance camera systems and the chilling effect this is having on people's freedom to go about their daily lives.

**Further action**

Reiterating the limits of my statutory functions I would respectfully suggest the following as possible further actions if you have not considered them already:

1. Raise a complaint with the Information Commissioner and seek his express advice - and possibly intervention - not solely on your individual circumstances, but as a broader area of policy and regulation in light of the vulnerabilities of MPs and their private lives.

2. Share your concerns with the Chief Constable of West Mercia Police in light of the response ordered by the former Home Secretary following the horrific murder of Sir David Amess MP in 2021 and request an assessment of your

security arrangements with particular regard to the risk of intrusive surveillance as you describe.

3. Contact the Security Minister within the remit of his Defending Democracy Taskforce as established by the Prime Minister last November, perhaps asking whether the matters you raise here will be addressed by the Taskforce. I have met with the minister in relation to the issues of intrusive surveillance and their relevance to the work of the Taskforce; your correspondence adds another significant dimension to this.

**Future regulation**

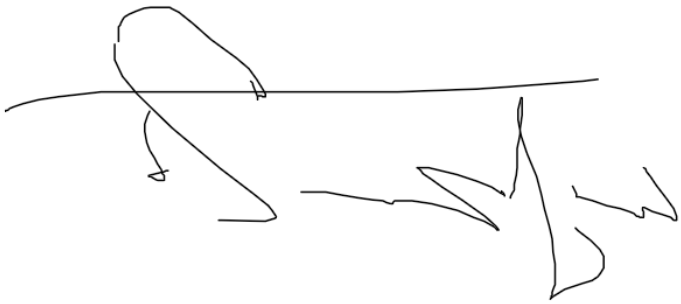
In my annual report to Parliament I have said that I do not feel the current regulatory arrangements go far enough in addressing the concerns of people around the increasingly intrusive nature of surveillance technology but that relying solely on the general protection of people's data rights cannot adequately address the many legitimate concerns that issue from the rapid advancement in AI-enabled biometric surveillance.

I recognise that the Code will be abolished by the Data Protection and Digital Information Bill and there are no provisions for its replacement, meaning there will be no specific legal instrument directly addressing the use of surveillance camera systems, by the police or at all. For this reason, I have commissioned a report by external academics into the residual risks and possible remedies for this situation and I expect initial findings of that report to be to hand imminently. I will share it with you if you would find that helpful and will copy this correspondence to the authors Professors Fussey and Webster.

Until such time as Parliament changes the legislation, I will continue to oversee compliance with the Code, encourage the adoption of its principles by all surveillance camera operators and provide advice in relation to the future arrangements to ensure that what is technologically possible is properly balanced with what is legally permissible and societally acceptable.

If I can be of any further assistance, please let me know.

Yours sincerely,



Fraser Sampson

Biometrics & Surveillance Camera Commissioner England & Wales

Email: enquiries@obscc.org.uk