



Baroness Williams, Minister of State for the Lords
Copy to: Rt Hon Michael Gove MP, Minister for the Cabinet Office
BY EMAIL ONLY

15 July 2021

Dear Baroness Williams

Risks and Considerations of Surveillance Camera Systems Under Extra-Territorial Ownership

I am writing to seek clarification and offer a way forward on a particular aspect of my functions which is attracting significant attention from both the public and internal partners. I believe it calls for a cross-departmental approach and have therefore copied this letter to the Minister for the Cabinet Office, Rt Hon Michael Gove MP.

Following a series of inter-related incidents and approaches for guidance from various quarters, I believe there is a pressing need to clarify the Government's position on the risks and considerations arising from the extra-territorial ownership of surveillance camera capabilities operating within the United Kingdom. Those incidents have included:

- the Government's decision in July 2020 to remove Huawei and its equipment from the 5G roll out programme and the continuing prohibitions on Chinese surveillance technology companies in the United States
- the report of the Commons Foreign Affairs Committee: "The UK's Responsibility to Act on Atrocities in Xin Jiang and Beyond" published on 8 July 2021 and
- the widespread public comment on the circumstances preceding the resignation of the former Secretary of State for Health & Social Care.

The risks and considerations in this field are complex and multi-faceted; I have tried to distil them according to my own functional areas. In respect of surveillance camera systems those functional areas are confined to England and Wales while my responsibilities as Biometrics Commissioner are UK-wide and are also relevant to some aspects of the points set out below.

Risks and Considerations

Following discussions with partners and stakeholders, it seems to me that the relevant areas can be set out in four inter-related strands:

Cyber and security

In some ways this is the most straightforward of the strands in that the risks of compromise to our surveillance camera networks are axiomatic and apply equally to all aspects of local and national infrastructure. Risks from cyber-attack generally are well documented and advice is readily available from the National Cyber Security Centre and Centre for the Protection of National Infrastructure. However, the proliferation of surveillance camera systems and advances in the attendant technologies possibly represent a new manifestation of an enduring risk. In particular, technical features such as systems-as-a-service (SaaS) and system-on-a-chip (SoC), together with the ease of future adaptation, the creation of systemic dependencies, 'function creep', the sectoral shift to 'cloud' technology and 5G systems and the rapidly increasing use of drones, both by private individuals and public bodies such as the police represent a renewed challenge for assurance, audit and compliance. Looking beyond surveillance cameras, the increasing interoperability /interdependency of systems that keep

our citizens safe raises further considerations about the provenance and practices of manufacturers and service providers. As the features of biometrics and surveillance systems become more sophisticated and further embedded in the infrastructure of our everyday lives they will demand renewed attention from us all.

Data protection and privacy

Not all surveillance camera-generated material qualifies as personal data for the purposes of the relevant legislative framework, but substantial areas do and the volume of the latter can reasonably be expected to increase in the future. Whether in the form of fingerprints, DNA profiles or facial metrics the international or cross-border processing of personal data is subject to clear regulation, safeguards and oversight. There are some aspects of the risks and considerations raised here that involve the framework for data protection and I will be raising them with the Information Commissioner, Elizabeth Denham when we meet this week. However, the impact on people's lives engaged by the risks and considerations is not confined entirely to matters of personal data and extends to areas such as the so-called 'chilling effect' on the extent to which people feel able to hold and express opinions, meet each other and demonstrate peacefully. These are elemental constitutional entitlements which also need to be considered in light of the perceived risks of non-UK owned and operated surveillance systems.

Economic considerations

It is clear that, when procuring surveillance camera systems, public bodies must assure themselves that the chosen system represents value for money for the taxpayer as well as functional efficacy and the financial reliability of the provider. Some of the camera systems being made available from outside the United Kingdom are highly competitive and cost-effective and are therefore attractive at both local and national level. It is unsurprising that some of the surveillance camera systems attracting attention are becoming popular with public services as they will probably excel in meeting the relevant criteria in the procurement scoring process. However, in light of the other elements, a legitimate question arises as to the appropriate weight that should be given to the economic considerations and the relative importance of some of the other areas set out here.

Ethics and international law

Perhaps the most challenging of the four strands is that of ethics and the rule of law. The importance of corporate values and social responsibility in democratic society has been understood and underscored for many years, with the provenance of products and processes at all stages of the supply chain now coming under closer scrutiny and often forming part of the due diligence of large corporations and their customers. Direct corporate complicity in the furtherance of human rights abuses *in the specific context of surveillance camera technology* has been raised directly by the House of Commons Foreign Affairs Committee (at paras 58-59). Having set out the evidence against which it reached its conclusions, the Committee goes on to make a number of recommendations which will be a matter for others. It is clear however that operators and purchasers of surveillance camera systems need direction and guidance on the specific surveillance-related issues, particularly where those operators and purchasers are local authorities; there is also a growing public interest in this aspect of surveillance policy.

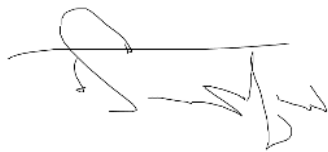
The Statutory Code

Ownership and operation of surveillance camera systems by entities that have their headquarters outside the United Kingdom is not of itself sinister, in fact many of the manufacturers and suppliers in

this field are trusted international trade partners. Assurance in the broad areas above comes primarily from a framework of regulation, standards and governance. In the context of surveillance camera systems this assurance includes the Surveillance Camera Code which, as you are aware, the Home Secretary has a legal duty to publish. Setting standards for their design and operation the Code covers surveillance camera systems in 'public space' (although I can find no express statutory provision limiting the Code's remit to this setting) and it is for the Government to designate which bodies must have regard to it. At this time those 'relevant bodies' are confined to local authorities and police forces. The incongruity of this aspect of the legislation with the reality of surveillance camera systems being operated across England and Wales has been pointed out by my predecessor in his annual reports and I will not rehearse it here. However, as the Code is to be revised and published for public consultation, it seems to me that there is an irresistible opportunity to address the risks and considerations above in the revised version of the Code and, at the same time, to review the list of relevant authorities who must have regard to it. For any revised list *not* to include Government departments in the future would surely require a very compelling case. As I mentioned in my recent letter to the Chair of the Commons Science & Technology Committee, I believe that the revised Code could also be incorporated readily and inexpensively by the Civil Aviation Authority into the licensing requirements for drone pilots.

Taking a broader view, I would welcome a cross-government discussion of the risks and considerations of extra-territorial ownership, acquisition and operation of our critical biometric and surveillance infrastructure, a discussion to which I would be very happy to contribute from the perspective of my specific roles.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Fraser Sampson', written over a horizontal line.

Professor Fraser Sampson
Biometrics and Surveillance Camera Commissioner