



OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Rt Hon Iain Duncan Smith MP

Copied to: John Edwards, Information Commissioner
Silkie Carlo, Director, Big Brother Watch
Rt Hon Baroness Williams, Minister of State, Home Office

10 June 2022

Dear Sir Iain

Risks to UK from Chinese State-Controlled Surveillance

I write further to the event at which we both spoke on the above subject earlier this week.

I would begin by endorsing your characterisation of the breadth and depth of the risks, their provenance and, most importantly perhaps, the urgency they now call for. The key question, as we on the panel agreed, remains what is to be done about them.

For my part, my correspondence with the relevant companies - and also with government departments - on this matter is all in the public domain but has yet to produce any discernible action. While the arguments deployed in this debate embrace a wide spectrum of issues, from my perspective as Biometrics and Surveillance Camera Commissioner the matter can be simplified to one of trust. The use of biometric surveillance by the state is a matter of increasing sensitivity and significant public concern - not just here but globally. As almost all of the technological capability for biometric surveillance is privately owned, the only way we will as a nation be able to harness the many legitimate uses of that technology in the future is in trusted partnership with trusted private sector partners.

In short, the people we trust - the police, fire and rescue, local authorities and the government itself - must be able to trust their technology partners, both in terms of security and of our shared ethical and professional values. And the publicly available evidence tells me that some of these companies - notably Hikvision and Dahua - simply cannot be trusted, partly because of concerns about the role they and their technology are believed to have played in perpetuating the appalling treatment of Uyghur Muslims as set out in the report of the Commons Foreign Affairs Committee last year (and recognised in the government's formal response), but also because of those companies' absolute refusal to engage with even the most cursory level of public accountability in response to those concerns.

The report by Big Brother Watch has corroborated what the surveillance community has known for some time: that almost every aspect of our lives is now under surveillance using advanced systems designed by, and purchased from, companies under the control of other governments, governments to whom those companies have data sharing

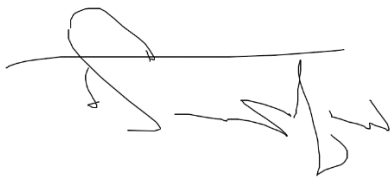
obligations within their own domestic legal framework. The proliferation of these systems means we have a public surveillance infrastructure built on 'digital asbestos' requiring both considerable caution when handling the products installed by a previous generation and, as a priority, a moratorium on any further installation until we fully understand the risks we have created.

I have been assured by ministers that these issues will be addressed in the Public Procurement Bill currently before Parliament and it is my sincere hope that any subsequent legislation will be sufficiently comprehensive, not just to address the letting of new public surveillance contracts, but also to reinforce the fidelity of our country's critical surveillance infrastructure in its entirety.

I will shortly be conducting a survey across police and local authorities to identify how many are relying on these surveillance systems but this will only inform a small part of the picture; what is ultimately needed is a full inventory across our critical national infrastructure.

To my mind this is not about interfering in another country's domestic affairs; this is about reinforcing the legitimate expectations in ours.

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