



OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Rt Hon Michael Ellis QC MP, Minister for the Cabinet Office
Simon Case, Cabinet Secretary

Copied to: Rt Hon Sajid Javid MP, Secretary of State for Health and Social Care

By e-mail to:

michael.ellis.mp@parliament.uk

cabinet.secretary@cabinetoffice.gov.uk

pssajidjavid@dhsc.gov.uk

21 April 2022

Re: Human Rights and Security Issues in Public Procurement of Surveillance Technology

Dear Minister and Cabinet Secretary,

Early in my appointment last year, I became concerned about the clear ethical and human rights issues involved in public procurement of surveillance technology from companies associated with atrocities in China. I have also been increasingly concerned at the security risks presented by some state-controlled surveillance systems covering our public spaces.

Insofar as the ethical and human rights considerations are concerned, the government has formally recognised that widespread, systematic human rights violations are taking place in Xinjiang, including extra-judicial detention of over a million Uyghur Muslims and other minorities, extensive and invasive surveillance targeting minorities, forced labour and suppression of births¹. This persecution relies heavily on surveillance technology as highlighted by the Uyghur Tribunal which found, among other things, that detainees were raped by police officers or by men who had paid to be allowed into the camp for that purpose. I have repeatedly asked one company, Hikvision, whether they accept that such things are even taking place and to clarify the extent of any involvement they have had in

¹ as set out in the Government's response to the Committee's Report, published 1 November 2021.

those camps as revealed by the Commons Home Affairs Committee last year. More than 8 months later they have yet to answer those questions.

In terms of security, public space surveillance is increasingly intrusive and modern surveillance cameras are built with the maximum functionality inside at the point of manufacture. This means they come with capabilities that can be switched on remotely in the future as and when they are needed, for example, the ability to pick up sound or read vehicle number plates. The more that surveillance camera systems *can* do, the more important it will be to reassure people about what they are *not* doing, whether that is in our streets, our sports grounds or our schools. This is increasingly difficult to detect technically and requires transparency and due diligence by all concerned in public space surveillance activity.

I have written to, and met with, ministers, partners and representatives from the surveillance industry on these issues. Most recently, I wrote to the Chair of the National Police Chiefs' Council highlighting the particular issues to which this situation gives rise in relation to policing. I was therefore encouraged to see reports over the Easter holiday that the Secretary of State for Health and Social Care has now prohibited any further procurement of Hikvision surveillance technology by his department.

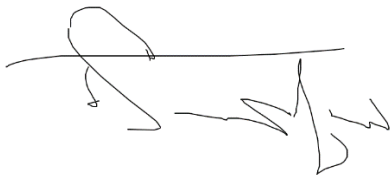
As the UN Guiding Principles on Business and Human Rights apply to *all* States and to *all* business enterprises regardless of their size, sector, location, ownership and structure, the rationale behind the Secretary of State's decision must apply equally across all government departments, devolved administrations and local authorities. They, and all businesses with whom they work, are under an obligation to respect internationally recognised human rights, wherever they operate. As the considerations at issue here are universal and not specific to a particular area of government there can be no justification for not extending this decision to all government departments and all local authorities and to include all other surveillance technology companies proven to have breached these fundamental and universal human rights obligations. I will shortly be publishing advice under the Home Secretary's Surveillance Camera Code of Practice (SC Code) to assist relevant authorities meet their human rights and ethical obligations in the use of public space surveillance. This approach is consistent with the

government's incremental, principles-based approach to regulation of the use of biometric surveillance technologies generally².

Transparency and governance are part of the 'golden thread' for human rights running through the UK government's guide to implementation³. Under the UN Principles, businesses must provide enough information to "evaluate the adequacy of an enterprise's response to the particular human rights impact involved"⁴. Without information none of us is able to carry out due diligence on either the human rights or security considerations on behalf of the public. For surveillance companies to refuse to provide necessary information is not only unacceptable; it also makes the provision of necessary public assurance impossible.

If we are to harness the significant benefits of emerging technology in this area in a lawful, ethical and accountable way, we need to build trusted surveillance partnerships. To do that, we must be able to trust our surveillance partners in respect of both the human rights and security considerations. If any government department has the necessary information to conduct due diligence in this regard, I would be interested to see it; if they have not, I would be interested to know how the human rights and security risks are being addressed.

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

² SC Code Para 2.

³ assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/522805/

Good_Business_Implementing_the_UN_Guiding_Principles_on_Business_and_Human_Rights_updated_May_2016.pdf, Principle 21

⁴ Principle 21(b) and para 21