For the attention of: Surveillance Camera Commissioner Fraser Sampson

British Security Industry Association
Anbrian House
1 The Tything
Worcester
WR1 1HD

Submitted electronically

8th September 2021

Re: Amendments to the Surveillance Camera Code of Practice

Dear Commissioner Sampson,

On behalf of the British Security Industry Association (BSIA) we are writing to submit joint comments in response to the Home Office's updates to the Surveillance Camera Code of Practice.

The BSIA is the trade association for the professional security industry in the UK. BSIA members are responsible for more than 70% of privately provided UK security products and services (by turnover) including the manufacture, distribution, installation and monitoring of electronic and physical security equipment and services, and the provision of security officer and consultancy services. Our members are industry professionals ranging in size from global companies to small and medium enterprises, offering quality products and services to a vast spectrum of end-users.

The BSIA comments to this Code of Practice are made in conjunction with consultation from its members including honorary member and former association Chair, Pauline Norstrom, founder of Anekanta Consulting, who have produced a hard hitting and disruptive in-depth response to the Code of Practice. Anekanta Consulting's paper calls for a root and branch change to the underlying legislation, the PoFA 2012, and for the recognition of the surveillance camera estate covering public spaces in the UK, as a "national security asset" whether publicly or privately owned and operated. The Anekanta paper forms part of our submission on the consultation and can be found here.

We agree with the updates and their intentions to use surveillance systems only for purposes that are clearly defined, lawful, ethical, and non-discriminatory, as can be seen in our latest published guide on the ethical and legal use of automated facial recognition. Whilst we support the Code and the solid set of principles providing the reader with a step in the right direction to transparency and compliance with relevant laws, there is a distinct lack of a "joined-up" approach to tackling the extent as to how much the Public are surveyed if at all, which may lead to a false sense of security.

As per Our BSIA recommendations to the amended Code of Practice are as follows:

1. The scope of the code should be extended to include all public and private operators whose systems monitor public spaces.
2. Private operators currently are not subject to Freedom of Information requests; however, the public can access images of themselves via subject access requests under the DPA 2018. A subject access request allows an individual to obtain information which can be used to identify them. However, there is no public disclosure of the location and use of cameras in the public spaces in which the individual can visit, whether subject to entry requirements or not. The development of a national database of camera locations should be required by law.

3. An open-source database of the locations of surveillance cameras covering publicly accessible spaces should be made available to the public. [E.g., such as apps which track aircrafts, marine travel etc., thus providing the British Public with more transparency].
4. The updates to the Code are superficial edits and do not materially alter the 12 core principles. Whilst the principles are sound, since the underlying legislation is weak, the Code can do more than advise of a duty to comply to a narrow user group which does not move towards strengthening a national security asset. The Police can gain access under legislation which already existed, but nothing in the Code makes that job faster, more efficient, or relevant to solving crime, or preventing crime. The latter being highly time sensitive, with events unfolding rapidly in real time.
5. The underlying legislation, namely Part 2 of the PoFA 2012 should be split out and made into a separate piece of standalone legislation governing the use of surveillance cameras in any publicly accessible place, also the analytics of images and the determination of facial biometric data from such images.
6. Section 12.3 only covers the live use of facial recognition the code should make specific reference to retrospective facial recognition for forensic purposes. If only live facial recognition is considered, the presence of a known terrorist could only be acted upon in real time whereas the build up to an attack can take weeks or months. The technology is needed to search image archives across multiple public and privately owned systems which are currently covered by different laws and guidance. The police can obtain imagery under RPIA, however there is no national image database nor any requirement for private operators to share their data.

In conclusion, whilst the amendments are necessary for a document which is 8 years of age, the technology has expanded far beyond a superficial update of the Code of Practice. With artificial intelligence and automated facial recognition software development and exponential use on the rise, the BSIA continue to be at the forefront of industry discussions and debates, in order to demonstrate its appropriate usage for ethical and legal purposes. The private sector for the video surveillance industry lacks clear and up to date regulation and guidance in the areas of AI and AFR and the BSIA, as the voice of the professional security industry, are willing to work with government on this important matter.

We look forward to hearing from you and for your further engagement.

Yours sincerely,

Mike Reddington

Chief Executive Officer
BSIA