Anekanta® Consulting

Surveillance Camera Code of Practice

Contribution to the response to the public consultation

Contents

Version Control

Date	Version	Author
8th September 2021	V 1.0 Feedback on the Public Consultation	Anekanta Consulting

Distribution

For issue to the Office of the Biometrics and Surveillance Camera Commissioner.

Purpose and scope

This document has been created by Anekanta Consulting. It forms part of a consolidated response from the British Security Industry Association (BSIA). Anekanta Consulting's founder is an honorary member of the Association and a former Chair. She is also a member of the BSIA's AI/AFR (Automated Facial Recognition) Special Interest Group which created a pioneering guide released February 2021 titled "Automated Facial Recognition - A guide to ethical and legal use", which has been highly acclaimed by the equivalent USA and EU Associations and Confederation of Associations (SIA - Security Industry Association and COESS).

Introduction

It is well known that the surveillance camera estate covering publicly accessible spaces in the UK is predominantly owned and operated by private companies. So much so, privately owned, and operated surveillance cameras out number public by a factor of approximately 70:1.[1]

The Surveillance Camera Code of Practice is an excellent reference document for relevant public stakeholders and goes a long way to advise private operators of best practice in line with current legislation. **However, the only relevant authorities which are duty bound by the Code are the Police and Local Authorities. Private operators are encouraged to comply, but this is not required by law[2].**

[1] This was established during the British Security Industry Association's research "The Picture is not clear" published in 2012 whereby its findings suggested there could be up to 6 million surveillance cameras in the UK in use for security purposes excluding cameras used on private dwellings.

[2] Protection of Freedoms Act 2012

Yet private operators are required to ensure that the security professionals monitoring the systems which cover a public space comply with the **SIA licencing rules, a legal requirement** under the Private Security Industry Act 2001. This is **regardless of whether the system is publicly or privately owned and operated.**

The private operator must comply with the DPA 2018 and UK GDPR to protect the privacy of the individual and a ICO Code of Practice exists pursuant to the DPA 1998 which also requires compliance with the law. However, the ICO's Code has not been updated since the adoption of UK GDPR and the DPA 2018. There is no current ICO guidance available for the use of surveillance cameras to cover publicly accessible spaces.

A very helpful ICO opinion on the use of live facial recognition software by private companies in publicly accessible places was published in June 2021. This relies heavily upon the DPA 2018 and UK GDPR, and the use of a DPIA[3] to assess the risk of infringing upon the rights of the individual. This is a very good step in the right direction.

The BSIA created a guide to the ethical and legal use of Automated Facial Recognition, anticipating the need for private sector guidance at the beginning of 2020, and published the guide in February 2021.

There appears to be a patchwork of overlapping legislation and guidance around surveillance cameras which cover publicly accessible spaces. **A unified, joined up approach** would be beneficial to national security and the day-to-day activity of protecting the safety of the public while respecting the human rights of the individual.

In the absence of joined up thinking in the legislation, the private professional security industry has already forged ahead to ensure that specialised image analytics technology can be used ethically and legally. The threat of the pandemic, the need for contactless interactions and the increasing terror threat is resulting in a private sector response, however there is **no overarching legislation in place which requires the use of standards, codes of practice and best practice guidance beyond voluntary adoption, and there is no clear and unified enforcement process to ensure compliance.**

To protect the individual's rights, they must be confident that their human right to privacy is protected, and this needs to occur through clear legislation, standards, auditing, and enforcement. **There should be transparency** such that the individual has access to the legal framework and all supporting standards to the extent it should be possible for an individual to make a choice to be monitored or recorded and categorised using surveillance camera images or not.

Planning for the future – big data

AI has been recognised during the pandemic as a valuable tool when used ethically and responsibly to analyse large data sets more effectively and more quickly than any human.

In the medical field, AI has been used effectively to discover new treatments for COVID, also to dynamically predict the demand for vital medical resources needed in hotspot areas.

In the case of the NHS, the national medical resource management was only possible since a) NHS is a public body, and b) has access to all hospital, treatment, and patient data relating to COVID and c) since appropriate legislative changes were made to allow access to medical data by providers of vital resources.

Although there are many systems in operation within the NHS, a harmonised approach was possible since there is a single authority responsible, together and relevant new legislation made it possible for widespread data analytics to

[3] Data Protection impact Assessment

occur. This served the national interest of the UK Government to keep people safe from the national threat of infection.

The use of AI is becoming more prevalent in the analysis of surveillance camera data feeds, but it cannot be used in any widespread analysis unless the systems are harmonised in some way, examples are a) single vendor solutions deployed across multiple installations, and user access is controlled properly b) managed via monitoring stations which have authorised access to multiple camera feeds together with the meta data c) public cameras monitored within security control rooms and per b) multiple feeds together with meta data are accessible.

Even if a harmonised central monitoring infrastructure existed, only live images of interest can be recorded by the control room, and in which case, the correlation between the data sources can only be done post-streaming for forensic review.

There is no national collective intelligence currently in existence which allows a determination of what happened leading up to an event by effectively reviewing events across multiple systems to track down perpetrators or planners of terrorist events.

This is due to the difficulty in accessing a multitude of surveillance systems with different recording formats, also in establishing two-way communication to retrieve footage from multiple systems retrospectively.

A paradigm shift towards cloud-based recording is advantageous because data is gathered into a storage centre which can be queried real time, rather than accessing hundreds of different systems with different formats. Accessing multiple systems is not impossible with appropriate interfaces which allow communication via proprietary protocols but there is a time delay, and not all users allow ingress from the outside.

There is no standard for video formats generated for surveillance of publicly accessible spaces, nor is there any requirement for video surveillance data which covers public places to be made accessible to any counter terrorism authority on demand. Forensic review can be undertaken using current legislation which gives access after the event, but the speed and effectiveness of the response is currently severely hampered by a lack of strategy in this area namely any move towards a national image database.

Prior to the pandemic, there was no joined up data strategy in the NHS in place and ready to activate, however necessity demanded it and it was done.

The NHS case example leads to the question “Why is the extensive surveillance camera estate still un-joined up and under-utilised when the national threat of terrorism is perpetual and growing?”

There must be an overarching strategy underpinned by legislation which specifically addresses the issue of access to surveillance camera images which cover public places.

Separate, specific, and detailed legislation for surveillance cameras should be created which would provide strong underpinning guidance for the creation of a Code of Practice which can be enforced. If this were done, not only would this improve the economy by creating a renewed drive towards refreshing and updating camera technology and its infrastructure, but the purpose of such could also become far more transparent and auditable in the public interest.

The UK previously led the world in its innovation in surveillance camera technology and through the standards and guidance to support its use. In recent times UK has not moved forward the underpinning legislation which states the UK’s strategy.

The private sector presses on, but this is in a silo to serve the needs of disparate customers.

A better strategy may join innovation with government policy in the way the UK Government's Innovation Strategy attempts to channel billions of development funds into academia and through to private enterprises for commercialisation. Surveillance cameras seem to have been left out of national innovation strategy yet are one of the most important resources which support the safety of publicly accessible spaces.

Core principles of the Code of Practice

The code provides a solid set of core principles for the scope and deployment of surveillance camera systems by local authorities which is a step in the right direction towards transparency and compliance with all relevant laws.

However, image data gathered in publicly accessible spaces, although a valuable national security and safety asset is not currently readily accessible by law enforcement or any authority as a time sensitive means of solving and preventing crime.

This is good news for the privacy rights of the individual and for those intent on causing mischief. Both can be content that "Big Brother" is most likely not to be watching at all.

This lack of joined up thinking also means that currently an individual is unable to determine from any central public source whether the publicly accessible area they frequent is covered by surveillance cameras. We are safe in the knowledge that the systems are in place to protect us, currently we don't know if they are there or not. It is currently a false sense of security, and a heightened sense of widespread surveillance and invasion of privacy by the government that does not exist.

The fundamental root cause of these issues is the lack of guidance in the core legislation which underpins the Code of Practice. Part 2 of the Protection of Freedoms Act 2012 (PoFA 2012), which requires there to be a surveillance camera code of practice is insufficiently detailed or relevant to the pace of change in technology, also the change in sophistication of those intent on harming others.

If Part 1 which covers the use of DNA and the national DNA database were copied and pasted and modified to be in line with the camera technology principles, the Code could move towards supporting the national interests from a strategic viewpoint. It is not suggested that this occurs, but it highlights the lack of detail in Part 2 vs Part 1.

It could be seen as contradictory that the PoFA 2012 legislation also regulates the activities of parking companies. In effect, a national security asset is regulated under the same act which allows the issue of a parking ticket by a private company to the owner of a car parked on privately owned land. Yet the national security asset, which also sits within private ownership is not guided in any level of detail to be useful as a future proof piece of legislature. This inconsistency in the level of detail, the approach to private and public concerns in the same piece of legislation cannot be right and needs to change.

Recommendations

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 accessible to the public. It is likely that half of the UK population generally do not feel safe walking alone in the hours of darkness due to the latent threat of being stalked or worse attacked. If it were possible to determine a safer route covered by cameras those intent of making the streets unsafe are more likely avoid those areas.
4. The draft 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 a sub-sample of the wider user group of a duty to comply, and 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. It is a good step forward to include the use of live facial recognition technology by the Police following the South Wales judgment. However, 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. Although the Police can obtain images under the relevant legislation, there is no national image database nor any requirement for private operators to share their data. This means that vital evidence may not be accessible or the delay in access could hamper effective action by the Police or Private Security Services. Public/Private sector partnerships are increasing in numbers, but this is due to the good practice of the security industry rather than any underlying legislation causing action.

End.