A National Surveillance Camera Strategy for England and Wales - Big Brother Watch Response

December 2016

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group that was founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this consultation Big Brother Watch is a member of the Surveillance Camera Commissioner's Advisory Council. The organisation has also produced a number of reports about the amount of CCTV cameras is the UK; these include *Are They Still Watching?* and *The Class of 1984*.

Key Points

- The Strategy's language must be easily understandable.
- The SCC's remit must be expanded to include all surveillance systems and the entire United Kingdom.
- The definition of "*relevant authorities*" must be widened to include more organisations.

Response

The Strategy and its objectives are laudable, but there are areas which we would recommend further consideration be given.

Language:

The bulk of the Commissioner's strategic vision is well articulated. However we have serious concern about the use of the phrase "*make them feel safe*". The use of the word "feel" in terms of safety is subjective and hard to define; different people have differing ideas of what makes them feel safe. Studies have shown that CCTV cameras make citizens feel safer, but no real evidence has been published to show that the majority of CCTV in our public and private spaces has had a measurable impact on safety or on crime. The only true measure of success should be whether or not surveillance systems are actually making people safer.

Some of the language throughout the document is vague and too reliant on buzzwords, which we feel is particularly unhelpful, often leaving the aims of the objectives un-quantifiable and the criteria needed to be met for success unclear. The following we believe need to be made clearer in order to be easily understandable:

- Objective 1: "*A clear road map"*.
- Objective 2: "*An early warning system to horizon scan technological developments*"
- Objective 6: "*There are 'soft levers' and incentives in place to encourage*".

- Objective 10: "*Greater synergies are established between regulators and those with audit and oversight responsibilities*".
- Objective 11: "*a single well publicised digital portal*".

Promotion of voluntary compliance:

The path to compliance for organisations which aren't deemed to be "*relevant authorities*" is an important tool but given the number of organisations this could potentially apply to, more has to be done to publicise adoption. Organisations should be required to display compliance on their websites and on other public facing publications. This could come in the form of a "seal of approval" or a visual clickable symbol which links to the Code.

We believe there is also value in requiring organisations to actively promote their adoption of the Code which could help raise awareness within their own sectors. Organisations should be encouraged to produce a press release about their compliance with the Code.

The Surveillance Camera Commissioner (SCC) should be required to maintain a publically accessible list of organisations which have voluntarily and mandatorily adopted and complied with the Code. Other bodies keep similar lists, for example the Civil Aviation Authority holds a list of all those who have a licence to use a drone for commercial purposes. This would give another avenue for those considering voluntary compliance to find out which other organisations had already done so.

We would also like to see the introduction of a system which allowed citizens and other stakeholders to measure how compliant particular organisations are with the Code. This could, for example take the form of a bronze, silver and gold ranking system. In this instance bronze would show that an organisation had only recently begun the process of compliance and that some staff are in the process of being trained, whilst a gold ranking would show that the organisation was fully compliant and all its operators are fully trained.

Objectives:

When looking more specifically at the objectives set by the Strategy it is clear that additional detail is needed.

Objective 3 mandates that information should be available to citizens and organisations to help them understand their rights and responsibilities in relation to surveillance camera systems. This provides a welcome step towards engaging more people in how surveillance camera systems are used in their communities.

It is a laudable attempt to increase transparency, but the process itself must be transparent if it is to succeed. Detail needs to be provided about how this objective will be achieved. If the source of the information is to be a "single point of contact" or "one stop shop" it must be clear which organisation will be responsible for publishing the information.

If separate material is to be published by each body which uses a surveillance camera system, efforts will need to be made to ensure a universal approach.

If this doesn't happen different information will be available to different people depending on which organisations they interact with. Citizens shouldn't be penalised because some organisations are more upfront about the rights and responsibilities of members of the public than others.

Objectives 4 and 5; the pro-active sharing of information about surveillance systems used by the police and location authorities, have the potential to create the most lasting impact of any of the objectives. That being said they also run the risk of being too easy worked around. Alongside these objectives the SCC must publish guidelines to set the standard for how, when and where the information pertaining to the operation of surveillance systems must be published. If this doesn't happen organisations could publish the information in obscure parts of their websites; making it more difficult for citizens to access.

There is also a risk that the information could be released with little publicity; meaning that citizens will have no idea where to look for it. To help generate a decent level of media attention and enforce a common set of standards, it might be worth considering the idea of an annual publication day. On this day all surveillance system users publish details about their system, its function(s) and any data sharing arrangements on their website. By establishing an annual day there would be a focus for all system users to have to adhere to publication. This method of an annual publication day is commonly used across many sectors.

Making sure that relevant information is published, well publicised, and properly accessible is only a small part of the work which needs to be done. The correct information will also need to be provided to ensure a helpful level of transparency. If the objectives are to be met the following information has to be published, as a minimum:

- The results of any trial of a surveillance system. These should be published alongside any stated objectives.
- Clearly worded objectives for every permanent surveillance system.
- Data related to the filming of offences by surveillance systems.

This will allow citizens to judge for themselves whether they think the surveillance systems in place are proportionate, necessary and achieving their stated goals.

The role of the Surveillance Camera Commissioner:

For the Strategy to work the remit and responsibilities of the Commissioner need to be expanded. The Commissioner's achievements up to this point should be applauded, but without reform many of the objectives he has set himself in his Strategy will be difficult, if not impossible, to achieve.

The current definition of "relevant authorities" for example is far too restrictive. The Protection of Freedoms Act (PoFA) mandates that only police forces and local authorities fall into this category and whilst they control large numbers of cameras, other bodies do so as well. Our 2012 report *The*

Class of 1984 found that English, Scottish and Welsh secondary schools controlled almost as many CCTV cameras as UK local authorities do.

The Commissioner himself has previously raised the issue of adding more bodies. In a letter to Brandon Lewis MP, Minister for Policing and the Fire Service, he noted that organisations, such as NHS Trusts, may benefit from being classed as "relevant bodies", this would be a sensible step[1]. In addition to this, at a minimum, the following types of organisations should be included as well:

- Central Government departments.
- Prisons and Young Offenders Institutions.
- State funded schools.
- Courts.

This move would have the added benefit of making Objective 7; ensuring that organisations involved in the critical national infrastructure comply with the PoFA, much more workable. At present the critical national infrastructure incorporates a vast number of organisations which have no obligation to self-assess. Reducing the number of bodies which don't have to self-assess, would help the SCC focus his resources. Without help the SCC won't be able to fulfil the goal of Objective 7 due to the sheer number of organisations involved.

At present the SCC only has powers to oversee organisations in England and Wales. The success of the Strategy will be hampered by the fact that in two of the four nations of the UK there is no way for the SCC to ensure the Code is being adhered to or that the objectives of the Strategy are being properly pursued.

This situation risks a two-tier structure developing with surveillance systems in Scotland and Northern Ireland not receiving the same level of scrutiny as those in England and Wales. If this were to happen it is highly likely that systems in England and Wales would be significantly more proportionate and effective than those in Scotland and Northern Ireland. The situation is further confused by the Scottish Government's insistence that CCTV providers in Scotland should abide by the Surveillance Camera Code of Practice; despite the fact that the Commissioner has no jurisdiction in Scotland.[2] The only logical way forward it seems would be to extend the SCC's remit to cover Scotland and Northern Ireland.

Perhaps most importantly the SCC must be given responsibility for overseeing the use of all surveillance systems in the UK. Big Brother Watch have called for this approach for a number of years. The current split in responsibilities between the Information Commissioner's Office (ICO) and the SCC we believe adds an unnecessary divide in an already complex patchwork approach to oversight. At the very least a joint code of practice should be published to fully clarify what elements

[1] Surveillance Camera Commissioner, *Surveillance Camera Commissioner's letter to the Minister for Policing, Fire and Criminal Justice and Victims*, 2nd November 2016, p. 1: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/571045/Letter-to-Brandon-Lewis-SCS-161102.pdf

[2] The Ferret, *Council breaking CCTV privacy rules, claims former worker*, 15th March 2016: https://theferret.scot/cctv-operator-claims-frequent-breach-privacy-rules/

the two organisations oversee. This would remove the need for both organisations to publish very similar but separate codes. This document should be placed prominently on the websites of both organisations. This may go some way towards properly clarifying the roles of the two organisations, but it isn't a real substitute for concentrating responsibility under one role.

The future:

Modern surveillance means much more than simply fixed CCTV cameras. Our public and private spaces can now be monitored by a vast array of different systems.

Body worn video, drones with built in cameras, facial recognition technology and portable surveillance systems are all being adopted and used by police forces, local authorities, private companies and private individuals, often with little understanding as to why they should be adopted or whether they are the right technologies for the job at hand.

The journey of CCTV over the past 20+ years should be seen as a warning. For too long and in too many cases CCTV systems were able to proliferate with no clear purpose, poor oversight, a distinct lack of accountability and no tangible proof of their value. This approach must not be allowed to repeat itself with any new surveillance capabilities, be they covert or overt.

As this Strategy points out, the need for privacy to be at the forefront of any purchase or installation of a surveillance capability or system is critical. With enhanced capabilities, enhanced protections must be adopted, not side-lined as unnecessary considerations.