SURVEILLANCE CAMERA COMMISSIONER

# Annual Report
2017/18

# Surveillance Camera Commissioner Annual Report 2017/18

Presented to Parliament pursuant to Section 35(1)(b) of the Protection of Freedoms Act 2012

**January 2019**

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at scc@sccommissioner.gov.uk

ISBN: 978-1-5286-0972-2

CCS1218140748

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

# Foreword

Dear Home Secretary

I am delighted to present my fifth Annual Report covering the period 1 April 2017 to 31 March 2018.

From the outset I will set out four key issues that are raised within the body of this report.

- The police use of integrated and highly sophisticated video surveillance platforms will continue to increase. The increasing pressure on resources and budgets is causing chief constables to look towards technology to support their law enforcement efforts. The balance between privacy and security when using new technology will continue to challenge law enforcement in its use, and lawmakers and regulators need to be robust and co-ordinated in supporting those efforts and challenging them when their use is deemed excessive.
- The overlap between police use of video surveillance platforms will become more entangled with that of private and commercial organisations. Clarity as to their use, intention and purpose is paramount if public trust is to be retained in the use of video surveillance camera systems by the police and others such as local authorities.
- This expansion in the use of video surveillance technology and integrated networks will only increase. I have harnessed, pro bono, the work and effort of leaders across the video surveillance industry to support the National Surveillance Camera Strategy for England and Wales. This report will demonstrate the breadth and depth of that work. However, without proper resourcing, this strategy will come under increasing strain. I have delivered a full and comprehensive strategic approach to the issue of public space surveillance cameras and secured the support of ten industry experts, all providing their expertise free of charge, to develop strategies, policies and best practice. My challenge to the Government is to recognise the value and currency of ensuring that public space video surveillance is properly and effectively managed and to resource this work, which is largely being delivered for nothing.
- The Home Office has committed to review the Secretary of State's Surveillance Camera (SC) Code of Practice. I have called for the need to recognise the burgeoning use of video surveillance platforms in many sectors, but particularly those in health, education and transport. The scale of organisations operating such systems in the public domain goes well beyond the limited range of 'relevant authorities' provided within the Protection of Freedoms Act 2012. That limitation is increasingly looking illogical and is rejected by the industry and operators themselves. The Government needs to have more confidence in the SC Code in achieving its purpose of driving up standards in what is increasingly an agenda that attracts significant public attention and debate.
- The use of public space surveillance camera systems pervades many aspects of our daily lives. Their presence and use continues to proliferate by agents of the state, the private sector and indeed by citizens themselves. Surveillance technologies continue to evolve at a pace that challenges established laws to keep pace. Meanwhile their inherent abilities to intrude upon a very broad spectrum of our fundamental rights and freedoms become far more detailed and sophisticated. Surveillance is much more than privacy and data. In acknowledging that threats to society are in themselves becoming increasingly complex and the resources that have the challenge to keep us safe are finite, it is inescapable that the picture

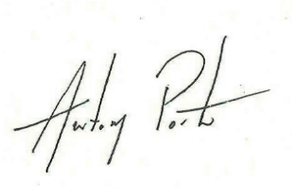
of public exposure to surveillance camera systems is far different and far more challenging than when my role was created in 2012. Civil liberty groups provide a valuable public service in raising concerns on such matters.

In seeking to meet the regulatory challenges involved I have secured broad support from many across the surveillance camera industry and other stakeholder experts. My launch of the National Surveillance Camera Strategy was and continues to be the key driver of a comprehensive 'full system' approach to deliver better and higher standards and lawful compliance in accordance with the SC Code. From the establishment of new industry standards for manufacture, procurement, installation, operation and information management systems, to civil engagement, education, cyber resilience, national infrastructure, operating tools, regulation and stakeholder engagement. The strategy has made, and continues to make significant progress in all areas.

Such progress is entirely due to the generous commitment and expertise so freely given by the ten industry experts mentioned earlier and many others from the stakeholder community. This report will demonstrate the breadth and depth of that work. However, without proper resourcing and commitment from the Government this work will come under increasing pressure, as indeed will public confidence in state regulation of such matters. There are indications of such concern currently arising in the context of facial recognition technologies. Having spent several years of raising concerns on such matters, on the increasing constraints of the Protection of Freedoms Act on my remit, and urging the SC Code to be updated, only now are there finally signs of movement by the Home Office. This is encouraging but hardly cause for celebration.

My challenge to the Government is to recognise the importance, value and currency of the National Surveillance Camera Strategy in ensuring public space video surveillance is properly and effectively managed, and to commit support to this work, which is largely being delivered using the expertise of volunteers.

I have a small team. I have no powers of inspection, audit or sanction, nor do I seek any. What I do seek, however, is greater understanding and tangible support on the part of the Government that, after all, is paid to serve the public, and a recognition as to the commitment made by those experts helping to progress my strategy, who are not. I do hope that the latter feel that my report adequately reflects their endeavours and the progress they have made.



Tony Porter
Surveillance Camera Commissioner

# Contents

# Introduction

I am required by section 35(1)(a) of the Protection of Freedoms Act 2012 (PoFA)[1] to prepare a report about the exercise of my functions and to provide a copy to the Secretary of State, who in turn lays the report before Parliament. Thereafter I am required to publish the report. This report covers the exercise of my statutory functions during the period 1 April 2017 to 31 March 2018. However, this report also covers any key issues that have come to the fore from that date until the date of publication.

I launched the National Surveillance Camera Strategy[2] in March 2017 to harness the rapidly increasing challenges, complexities and demands facing my role within a more coordinated framework, supported by structured delivery plans. The strategy is the key focus for the delivery of my functions and continues to receive excellent support from across the surveillance camera stakeholder community. In that regard it is intrinsically linked to my everyday work. This report reflects the ambitions and outputs of that strategy in its first year.

The strategy has recently (March 2018) had its first annual review and by necessity is a prevailing theme throughout this report.

The strategy is aimed at joining together the disparate elements of the 'video surveillance camera community', from manufacturers and installers to end-users, to drive up standards so that public confidence in this type of technology can be maintained. Manufacturers rarely talked to installers or consultants. Operators were unsure as to what equipment to buy. The police and local authorities were not getting the benefits from joined-up working. The existence of standards was present but not visibly utilised. The citizen was left not knowing the capabilities of this new technology or if indeed they want it.

The strategy provides a vehicle to improve standards, which was one of the key aims of the legislation – the PoFA – that introduced the role of the Surveillance Camera Commissioner. The delivery of the Buyers' Toolkit[3] within this reporting year is a major deliverable within the strategy that is aimed at enabling purchasers of such equipment to get the right kit to do the right job. I also believe that it will influence manufacturers to raise their standards as buyers begin to demand better quality equipment, improved cyber protection, and so on.

The strategy is also aimed at providing democratic oversight, through this report, to Parliament. It will demonstrate where the strategy has succeeded and also where greater effort is required. It will make it easier to see whether the vast cost that is channelled into such technology is delivering value for money. Or indeed whether my role, a global first, provides sufficient evidence that standards are being driven up and the relevant authorities (local authorities and police forces) are complying with the requirements of the PoFA.

The reader will see the enormous challenges that my office has taken on despite restricted and finite resources. I am delighted to receive continued support from the Home Office, yet if this work is to achieve what it is capable of I am certainly in need of additional resources, for the reasons below.

---

1 http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
2 https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales
3 https://www.gov.uk/government/publications/surveillance-camera-commissioners-buyers-toolkit

The existence of video surveillance systems on the streets of England and Wales is often described as ubiquitous. The shift from analogue to digital equipment and from simple image capture to augmented technology has been rapid. Last year I reported that the most recent estimates for the total spend on video surveillance cameras was £2.25 billion. We are seeing the increasing use of automatic facial recognition (AFR), unmanned aerial vehicles (UAVs), automatic number plate recognition (ANPR) and body worn video cameras (BWVs).

Readers of this report will be interested in global shifts in the use of such technology. Whereas the UK was usually feted as the most surveilled country through video technology, in the world we are seeing China (and many other countries) expand their technology. One such programme known as 'Sharp Eyes' in the province of Xionping combines video surveillance technology and AFR. Its capability in terms of monitoring its population is growing – from people who are blacklisted from certain areas to commercial purposes. A reported 176 million cameras are now operating across China. Its police forces on the outskirts of Beijing are trialling facial recognition sunglasses. They are used to check travellers against government blacklists and their cost is apparently as low as £400 per unit. These developments throw down an obvious challenge to society: To what extent is it willing to sacrifice its personal freedoms for security? Whilst this is a perennial debate that I do not see drawing to a conclusion any time soon, I am clear that a society cowed by ubiquitous surveillance technology monitoring our every movement, cross checking reference databases to enable the state to monitor its citizens, is not an approach supported in this society.

I have been active throughout these 12 months in highlighting the issues and challenges that such technology will present to the citizen and the Government in terms of regulation. The landscape, at the time of writing, remains complex concerning where exactly responsibility and accountability from a regulatory perspective sits. The new Data Protection Act 2018 will provide stronger powers to protect against data processing abuse. However, it does not provide a holistic approach to regulating the actual use of surveillance. Nor does it alone provide a legal basis for the use of such surveillance. The use of intrusive surveillance is also covered by common law jurisprudence, the PoFA and the Regulation of Investigatory Powers Act 2000. At the time of writing civil actions against South Wales Police and the Metropolitan Police Service are being pursued by Liberty and Big Brother Watch respectively in regard to their use of AFR technology. These actions challenge the legality of its use and undoubtedly the outcome of those hearings will be significant in the ongoing consideration of their deployment.

The Home Office has produced the long awaited Biometrics Strategy.[4] This strategy proposed to establish an oversight and advisory group that will seek to provide advice to the Government and the police about the use of biometrics and facial imagery. I have been clear about the challenges that this technology faces and I would refer the reader to my speech made at the Taylor Wessing Annual Data conference earlier this year,[5] which sets out the arguments and challenges to the use of this equipment.

The strategy does represent recognition by the Government that the rapid march of such advancing technologies requires a degree of harnessing across policy and lawmakers. I am also delighted that the strategy recognises the requirement to review the Secretary

---

4 https://www.gov.uk/government/publications/home-office-biometrics-strategy
5 https://www.gov.uk/government/speeches/speech-to-the-annual-data-privacy-conference

of State's Surveillance Camera (SC) Code of Practice and ensure that it properly and effectively reflects the changing environment. This was a recommendation that I made in the *Review of the surveillance camera code of practice* (February 2016).[6]

You may recall I commented in last year's Annual Report:

> *"New technology challenges the legal basis or legal justification of this technology. Automatic Number Plate Recognition Systems (ANPR), facial recognition systems and other forms of integrated technology are becoming hardwired into our society."*

I have frequently engaged with the Home Office relating to arguments supporting a statutory framework for ANPR. Coupled with the proposed action from Big Brother Watch and Liberty relating to the legality of the use of AFR techniques these arguments appear to expand to the use of other surveillance systems capable of utilising artificial intelligence. These dynamics will continue to reverberate as technology continues to accelerate, from facial recognition to gait and voice recognition. From systems that are linked, to sensor and video surveillance technologies with complex reference databases, these are arguably capable of being more intrusive than authorised covert surveillance.

I have made repeated calls to Ministers and the Home Office to give further support to the SC Code, which at the time of writing remains the only legislation actually specifying a regulatory role on the use of AFR and advancing surveillance camera technologies. I will strenuously support the strengthening of this SC Code during the aforementioned review. I will particularly look to the Government to continue to expand those organisations that must statutorily comply. It is ironic that the Government will introduce video surveillance systems into abattoirs for the betterment of animal welfare but has rejected my repeated calls for the NHS to be made a relevant authority within the PoFA. Millions of patients, arguably at their most vulnerable, are exposed to ever increasing surveillance technology from drones and BWVs to AFR. I have been told by the Government that the new Data Protection Act 2018 provides the relevant reassurance; this is not in my view persuasive. Why would the Government not seek to apply the highest standards of surveillance management across all public sector agencies, particularly those that exercise responsibilities under human rights legislation? Additionally, I believe that the Data Protection Act 2018 does not provide a robust statutory framework for all the surveillance camera platforms mentioned above.

Further, I continue to argue that organisations such as Transport for London, the Highways Agency, education establishments, rail franchises, and cameras that cover the critical national infrastructure should, as an absolute minimum, be included as relevant authorities within the PoFA. I can make no stronger argument than pointing out that it is an absolute nonsense that the smallest of parish councils in England and Wales must have regard to the SC Code yet the operators of huge and intrusive systems that have the potential to invade upon the everyday life of many of our citizens do not. In passing the PoFA and introducing the SC Code the commitment was made to keep the SC Code under review and expand the list of relevant authorities incrementally. The argument for expansion is now pressing.

---

[6] https://www.gov.uk/government/publications/review-of-the-surveillance-camera-code-of-practice

In the *Review of the Operation and Impact of the Code* (February 2016) I called for a single Code of Practice to be introduced covering the operation of video surveillance systems (Recommendation 9). This was to elimate the confusion caused by there being two codes of practice in this area. The SC Code and ICO's code – *In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information*.

You will read in Chapter 4 relating to the police that this confusion still remains. The Government's own post-legislative review of the PoFA[7] (part 2 paragraph 11) concurred that the duality of codes has caused confusion.

I sincerely hope that, given the traction that the National Surveillance Camera Strategy has gained we, as regulators, will be able to harness a more streamlined approach by producing a single Code of Practice, with a single harmonised approach for the lawful, efficient and transparent use of such systems.

Global interest in the role of Surveillance Camera Commissioner has increased this year. I have seen an increase in interest in public space surveillance in Berlin post the terror attacks that claimed 12 lives in December 2016 when a truck was driven into a crowd at a Christmas market. I have conducted media interviews for national television and had requests to make speeches concerning such issues from Germany, France, South Africa and Japan.

The Government's approach to creating an independent Surveillance Camera Commissioner has been recognised as far afield as Victoria, Australia, which is seeking to introduce legislation concerning the use of AFR and oversight through the offices of an independent commissioner.

As part of my national strategy I have commissioned a horizon-scanning workstrand (see Chapter 2) aimed at providing regular briefings to my Advisory Council (and in turn the Government) on new technology. I intend to use this information right across the strategy, not just for operators but also for fellow regulators to provide any information and support that might be valuable in their role.

The initial report has informed further development of the strategy and was presented to Home Office Policy to ensure visibility to new and emerging challenges.

The reader will also see the early fruits of the citizen engagement strand (see Chapter 3) where, with the leadership demonstrated by the Centre for Research into Information Surveillance and Privacy (CRISP), the first *Question Time* styled event was held in February 2018 at London School of Economics. It was a challenging event where regulators, chief constables and civil liberty groups took questions from the public and outlined their views and perspectives. This debate can be listened to online.[8] We plan more events during the coming reporting year.

The perennial challenge to government policy makers and the regulators is to demonstrate versatility and coherence in facing these challenges. The concept of the role of the Surveillance Camera Commissioner very much envisaged these challenges – how is it possible to legislate and indeed regulate in the face of technology that changes daily?

---

7 https://www.gov.uk/government/publications/post-legislative-scrutiny-of-the-protection-of-freedoms-act-2012

8 https://www.stir.ac.uk/about/faculties-and-services/stirling-management-school/our-research/research-areas/management-work-and-organisation/current-projects/

So this report will take a different shape from previous annual reports. It will lead you through the National Surveillance Camera Strategy and enable the reader to understand more fully how this complex area of business is progressing from a regulatory perspective, and also in terms of the new and dynamic challenges that we face. The only strand that does not have a dedicated chapter is the one focused on the critical national infrastructure. We have worked hard with colleagues at the Centre for the Protection of National Infrastructure (CPNI) but many of these infrastructures, through necessity, are secretive around their protective measures. The approach of the CPNI, however, recognises that although secrecy may be an absolute requirement, this does not mean that standards for the use of public space surveillance cameras should not be demonstrably high. The CPNI has already achieved many of their deliverables in their workstrand.[9]

The Government introduced the PoFA and the SC Code to improve standards and increase confidence in the use of public space surveillance in England and Wales. The significant highlights of the year are reflected below.

- Extensive survey of all police forces in England and Wales to understand their surveillance camera 'footprint' and how they are complying with legal requirements under the PoFA and the SC Code.
- Building momentum behind the National Surveillance Camera Strategy for England and Wales to deliver:
    - the first Question Time style event to enable serious debate on how surveillance cameras and associated technology impact on citizens;
    - a series of national workshops aimed at local authorities to advise them how to comply with the 12 guiding principles in the SC Code;
    - the first horizon-scanning report to enable us to peer into the future at how surveillance cameras may develop;
    - cybersecurity considerations across all strands of the strategy from standards to training; and
    - developing a new 'Buyers' Toolkit' – an easy-to-follow guide for non-experts (aimed at small to medium enterprises) that are thinking about buying a surveillance camera system, and want to ensure that they buy an effective system that does what they want it to do.
- Formulation and first meetings of the ANPR Independent Advisory Group, which I chaired, to scrutinise the deployment and operation of automatic number plate recognition as a surveillance tool. It comprises specialist external interests as well as the police, the Information Commissioner's Office and the Home Office.
- The emergence of automatic facial recognition as a viable technology used by both state and private organisations.

The challenges to civil liberties arising from new and emerging surveillance camera technologies are significant. I have identified the pending legal actions and we await their outcomes. Facial recognition has dominated media focus throughout the year and will continue to do so over the coming year. Additionally ANPR and intrusive video analytics are increasingly present across society. They are not going to become less sophisticated

---

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704483/Strategy_plan_7-_critical_national_infrastructure.pdf

but more sophisticated. We live in times where the spectre of terrorist attacks confronts us daily, and the pressures on our police and intelligence services has never been greater. It is acknowledged that video surveillance technology provides operational benefits to those who are charged with the responsibility to keep us safe, and they also bring an added dimension to customer convenience. However, their use does continue to raise challenges when seeking to balance security and privacy.

Informing the public is key in my view. I will be holding further public debates and engagement throughout the year as part of my National Surveillance Camera Strategy to allow the public to have their say – to inform me, the Government and fellow regulators as to their views and opinions.

I set out within the strategy to increase the visibility of new and emerging technologies. I am committed to continuing this debate.

## Resources

For the reporting year my resource allocation comprises an annual salary budget of £195,664 and £50,000 for non-staff pay. This largely comprises four members of staff. My own salary is funded by the Public Appointments Committee.

It is appropriate to consider the issue of resources that support my role. Throughout the reporting year I have operated at a 50% reduction in staffing level due to transfers from the office on promotion and the delay in recruitment to backfill those posts by the Home Office.

Whilst the Home Office and the Government support the strategy, and given that its very objective supports the Home Office single departmental plan[10] – particularly in cutting crime, countering terrorism, and protecting vulnerable people and communities – the extent of resources attached to this work is minimal at best. Given the limited resources, the failure to ensure backfilling of staff has placed a tremendous strain on the remaining personnel.

In last year's Annual Report I referenced the £2.25 billion spend on the video surveillance industry. The reader will see throughout this report how the landscape is changing – from the introduction of the new Data Protection Act 2018 to advancing technology (facial recognition, biometric analysis via video systems) and the increasing complexity of workloads across the regulatory landscape.

This expansion in use of video surveillance technology and integrated networks will only increase. I have harnessed, pro bono, the work and effort of industry leaders across the video surveillance industry to support my strategy. This report will demonstrate the breadth and depth of that work. However, without proper resourcing, this strategy will come under increasing strain. I have delivered a full and comprehensive strategic approach to the issue of public space surveillance and secured the support of ten industry experts working free of charge to develop strategies, policies and best practice. My challenge to the Government is:

- to recognise the value and currency of ensuring that public space video surveillance is properly and effectively managed; and
- to resource this work, which is largely being delivered at zero cost.

---

[10] https://www.gov.uk/government/publications/home-office-single-departmental-plan/home-office-single-departmental-plan--2

# Chapter 1 – National Surveillance Camera Strategy for England and Wales – Standards

This strand of the National Surveillance Camera Strategy[11] is led by Alex Carmichael, Chief Executive of the Security Systems and Alarms Inspection Board (SSAIB). Alex is supported by a strategic Standards Group, which spans the whole spectrum of the industry. The focus of the Protection of Freedoms Act 2012 (PoFA) is to ensure that public support and confidence in public space video surveillance systems is maintained and enhanced. This can only be done if standards are set, applied and maintained. To that end you will note that last year I reported that I had published a set of relevant standards on my GOV.UK website[12]. Whilst this is a first step it is important to recognise that it is only that. How are the systems policed? Does it matter if a British standard or European/ International standard is met? What does it mean to the buyer of a surveillance system and more importantly the public, who are subject to that surveillance?

Principle 8 of the Secretary of State's Surveillance Camera (SC) Code of Practice provides the basis for the work of the Standards Group:

> *"Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards."*

So, what is the Standards Group working on to support the National Surveillance Camera Strategy?

The first is best practice guidance for in-house monitoring centres, monitoring their own camera systems. Such centres do not have to meet any requirements, except under the Data Protection Act 2018. It was felt that providing best practice guidance would aid in-house monitoring centres to understand how they should secure, manage and operate such a centre. It will also help them to meet the principles within the SC Code. The guidance will be split into two parts:

- a mandatory element, which the monitoring centre should meet; and
- a desirable element, which will enable the monitoring centre to meet the published standards.

This guidance is being put together in conjunction with the National Association of Surveillance Camera Managers (NASCAM) to whom the Standards Group is very grateful. I anticipate that completion will align with the projected dates highlighted within the delivery plan.

---

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704449/Strategy_plan_1-_standards_and_certification.pdf

[12] https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry

In previous years I have focused on the success of the introduction of third-party certification[13] for operators of video surveillance camera systems. I am keen now to focus on the complex supply chain to develop linkages between the operator and the rest of the process.

With regards to installers we have decided to use the term 'service provider' to mean integrator, installer or maintenance company, as this is the term used in the Surveillance Camera Commissioner's Buyers' Toolkit (June 2018). For service providers we are putting together requirements based on current good practice, using the applicable standards stated on my website.[14]

These will enable third-party certification of service providers to the applicable standards and current (to be amended) service requirements taken from the National Police Chiefs' Council (NPCC) *Guidelines on Police Requirements and Response to Security Systems*, Appendix S, clause III.[15]

The standards strand is using the NPCC policy for the draft service requirements, as these are what many video surveillance service providers are currently certificated to. Again I anticipate this being delivered on schedule as per the above delivery plan. A wider ambition is to enable all types of monitoring centres to meet the necessary standards and, if they wish, to have third-party certification. Running through this approach, like a golden thread, is the development of a recognised branding that is aimed at providing assurance to the public that the recognised standards are being followed. This brand will carry the Surveillance Camera Commissioner's (SCC's) logo, which is already nationally recognised.

There are two issues that have come to the forefront over the past year. The first is the introduction of the General Data Protection Regulation (GDPR), which is included into UK legislation as the updated Data Protection Act 2018. Strong data protection (privacy) is something that the standards strand is very conscious of:

- for video surveillance manufacturers it means privacy by design;
- for service providers it means reviewing how they process personal data;
- for CCTV monitoring centres it means reviewing their current data protection procedures, storage and retrieval procedures; and
- for consultants it is reviewing how they manage the personal data they hold on behalf of their clients.

The standards strand has been looking at cybersecurity, for the various workstreams within the strand. Mike Gillespie an industry specialist and President of the Centre for Strategic Cyberspace and Security Sciences (CSCSS), Cybersecurity, Cybercrime, and Cyber Intelligence (C3I) Initiative has the cyber lead for all strands of the strategy. In terms of standards both Mike and Buzz Coates (IP CCTV Business Development Manager at Norbain) have been working hard to ensure that the message gets out that cybersecurity needs to be included in all aspects of a surveillance camera system. Cybersecurity is something that I am passionate about and the strand is working hard to incorporate the appropriate guidance on cyber into my guidance and requirements.

---

13 https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme
14 https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry
15 http://www.securedbydesign.com/security-systems-policy/

The cybersecurity strand and cross-workstream function have been very busy. Much work has been carried out to push the message of driving up standards; this has been equally focused on manufacturers, installers and operators.

- **Manufacturers** to help to promote and explain the vital nature of 'secure by design' and why it needs to be the industry standard.
- **Installers** to help to promote and explain the absolute necessity of 'secure by default' and the key role they play in making sure that the equipment that manufacturers have shipped as secure is installed and left securely.
- **Operators** to help to promote and embed the knowledge that adding networked systems to their estate means adding to the 'internet of things' and with that comes the responsibility to secure it through its life cycle.

Part of the work is making sure that all of these groups understand why it is so important to get this right, and why it matters so much. Networked systems:

- can enable cyber attacks, including distributed denial of service and botnet[16] attacks that can affect a wide range of public platforms;
- are gateways to organisations and all of their systems, not just security systems;
- represent a potential soft underbelly or easier route in when not effectively protected; and
- the interconnected nature of our business ecosystems means that there is a threat to our critical national infrastructure through supplier networks.

Key successes of the work on cyber embedding have included the formation of a working group of manufacturers. These manufacturers are collaborating transparently to design standards for security systems that manufacturers can be measured against and continually work to improve upon. The anticipation is for a draft standard to have been produced by financial year 2019.

Future activities planned include setting up similar working groups to involve installers, system integrators and consultants, with a view to creating similar, complementary standards and continuing to build momentum behind a programme of continuous improvement, as with the manufacturers.

The cyber message will continue to be widely relevant and so the work will continue across the workstreams and functions, and in particular through the next phase of horizon scanning to ensure that I continue to keep a finger on the pulse of current security events and needs.

Video surveillance consultants is also an area that the standards strand is working on, in conjunction with the Association of Security Consultants (Jon Laws, Director, SafeGuard Security Consultants and Andrew Sieradzki, Director of Security and Technology, Burrohappold Engineering). One of the first issues to be addressed is what is the definition of a consultant? To inform this discussion the workstrand proposed that the requirements for a video surveillance designer are developed. My aim is for a simple recognition of the

[16] A botnet is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system.

role against standards to continue to provide a constant theme that runs throughout this complex industry. This strand objective has been deferred by six months to take account of the complexity of available routes open to compliance.

Through the former Centre for Applied Science and Technology (CAST) now the Defence Science and Technology Laboratory (Dstl), the strand is looking at new and emerging technologies and, where practical and possible, seeking to develop standards or guidance for such technologies. Not an easy task, as many of the requirements for new technologies have privacy issues that should be considered in conjunction with the Information Commissioner's Office (ICO).

This will give the standards strand a framework to base technical guidance on a strong privacy foundation. Facial recognition has become a key focus throughout the reporting year and some good work is already beginning to emerge from this work.

The issue of cybersecurity will run through this report as a constant topic. I am delighted to say that under Alex Carmichael's leadership this strand is moving towards developing a baseline cyber standard for manufacturers. Following the Washington cyber attack[17] immediately prior to the inauguration of President Trump, the vulnerability of video surveillance systems to this kind of attack have come under the spotlight. These are important steps and I look forward to reporting more fully on this initiative next year.

My standards strand and, indeed Advisory Council, had repeatedly raised the issue of an absence of a British Standard for the use of body worn video cameras. I am delighted that, as a result of collective effort across the industry and British Standards Institution, in June 2017 we saw the introduction of BS 8593 – a code of practice for the deployment and use of body worn video cameras. I am, however, frustrated that I have not been able to move quicker and support additional work that is a priority – harmonising work and best practice guidance for the use of drones, facial recognition, video analytic technology to name but a few.

So, the standards strand is exceedingly challenging with a diverse workload and many areas of focus, yet all the participants give up their time for free. However, they all have the same goal in supporting my statutory function in ensuring that video surveillance meets end-users needs by providing privacy by design, supported by a standards and guidance framework.

[17] https://www.cybersecurity-insiders.com/cyber-attack-on-washington-dc-public-cctv-network/

# Chapter 2 – National Surveillance Camera Strategy for England and Wales – Horizon Scanning

I am indebted to Neil Cohen (formerly Home Office Centre for Applied Science and Technology (CAST) and now Defence Science and Technology Laboratory (Dstl) who has led on the horizon-scanning strand of the National Surveillance Camera Strategy[18]. Neil has been a continuous source of advice and support in the ever increasingly complex world of video surveillance technology and the challenging issues of 'what does the future look like?'

It will be helpful first to outline a picture of how technology is developing in the world of video surveillance systems.

## Technological Developments

CCTV is in itself a misnomer. It is no longer a stand-alone closed-circuit system and has not been for some time. The understanding needs to widen considerably to reflect this change. In the near future, we will have mass streaming of video data from static, drone, body worn video cameras and mobile phone sources to online cloud storage; a long way from the more conventional static digital video recorder.

The technology available for surveillance purposes is developing at an ever increasing pace. Developments in artificial intelligence (AI) show strong signs of dramatic improvement in the near future. This may mean that we will no longer need the classic CCTV system where a human being views an image on a screen and acts accordingly. In the longer term it is not impossible to envisage a system with no human operators in the loop at all, analysis of the images being done automatically. What are the implications for public trust in the system? Currently the final decision is made by a human operator. What if this is no longer the case? It may soon be the case that an AI system can make more reliable decisions than a human operator, but will this be acceptable to the public?

This raises the question concerning safeguards. As opportunities to create new methods of deploying such technology become available – do our laws and regulations provide sufficient safeguards against misuse? The new Data Protection Act 2018 certainly provides a strengthening of privacy rights but I believe does not of itself provide the legal justification for conducting such surveillance in the first place.

An example of one of the big drivers for surveillance cameras could be the increasing use of driverless cars. These vehicles will have 360° vision with the provision to store those images. Also the data may be transmitted to:

- the owner (who may be an individual or the company providing a fleet of vehicles for hire);
- the insurance company; or
- a central monitoring service.

---

[18] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704447/Strategy_plan_2_-_horizon_scanning.pdf

This has a range of implications – personal data, privacy, policy for investigations (more data available, but where is it/how to get it?). Camera technology is almost certain to change over the coming ten years. Imaging systems will routinely have multi-megapixel capability and begin to approach the absolute resolution of film. In fact the technology is already here – widespread take-up is mainly limited by cost (including the costs of upgrading legacy connection infrastructure). The technology will:

- be able to view and record in 3D;
- have considerable front-end capability to perform on-board video analytics;
- have considerable built-in redundancy giving improved reliability; and
- have the ability to view and record scenes using light that is outside the video spectrum (for example, infra-red and ultra violet).

It may also be possible to apply narrow band filtering that would turn networked video surveillance systems into networked sensor systems for a variety of threats.

Radio frequency identification (RFID) tags (and other similar devices) could be linked to video surveillance for tracking purposes. In the more distant future, a person's electronic footprint could be linked to video surveillance via the internet of things to provide a ubiquitous tracking capability.

There are also many new sources of imagery, beyond static video surveillance systems, for example, body worn video cameras and drones. The threat from drones is well documented. There are reported incidents of them being used to drop drugs into prisons, conduct unauthorised surveillance and invade individual privacy. At the same time the immense opportunities presented by this technology must be embraced by a forward facing, technologically friendly society. The issue refers back to that thorny debate – privacy versus security.

The future will see the introduction and adoption of augmented reality. The initial Google glass was not seen as a success, but this was probably a setback for the technology rather than a death knell. This technology has a number of implications when combined with large databases that are readily accessed via the cloud (the big data agenda). The potential for automatic facial recognition is already with us and the identity agenda is liable to be a major driver of developments. A potential example is the ability to conduct non-facial recognition biometrics from a distance, such as gait analysis and iris recognition.

There are bandwidth issues attached to the expansion of all-embracing surveillance technology. The more information that is recorded and distributed the greater the burden on the radio spectrum allocated for the purpose. This is not an infinite resource.

These other data sources/databases that will be used alongside the imagery also need to be accurate and trusted, and perform to defined standards. The Secretary of State's Surveillance Camera (SC) Code of Practice that I oversee refers to requirements in this area. However, the size and scale of these issues will require a fundamental rethink as to how the Government intends to regulate the widening capabilities and capacities of the technology against the static resources applied to regulation in this area. In the introduction to this report I referred to the limited resources afforded to my offices. I continue to urge the Government to consider these issues and ensure adequate support and resources are provided into this important area.

There will still be a need to be able to specify the minimum quality of equipment that must be met when systems are implemented. Again the SC Code firmly places responsibility upon the shoulders of the Surveillance Camera Commissioner in this regard. Requirements under the Data Protection Act 2018 (DPA) for "*privacy by design*" and "*privacy by default*" will provide firmer guidance around the standards to be developed, but they still need to be developed and engagement across industry employed. I am pleased to say that my national surveillance camera strategy is engaging across all these areas – particularly cyber.

The pace of change of technology makes systems become obsolete at an increasingly fast rate. Systems are becoming increasingly dependent on software for a whole host of reasons and suppliers simply stop supporting certain versions after a short time when compared to the expected life of a system. The video surveillance community is too small to influence the policies of the big software providers.

There are technological implications for all aspects of the video surveillance system – not just the 'front-end' camera, but also the transmission, storage and analysis – all will advance.

At the 'back end' of the system is often the police/criminal justice system. Will they have the capacity and capability to deal with this flood of new information? What is the purpose in collecting it if it cannot be used effectively?

Many of the developments and deployment of advanced analytics technology will be from commercial sources rather than the Government – the capabilities produced by Google/ Amazon and other technology companies will advance at a greater rate and be far more sophisticated than anything produced by the Government or 'relevant authorities' (which have much smaller resources at their disposal). So where does the risk to individual privacy really lie going forwards? Not with the state, although infringement by the state of the rights of its citizens quite properly attracts criticism. It is easy to be blinded by technology. However good the technology, there is still a need to get the basics right, for example, the requirement, specification, design, installation and operation. Replacing a poorly installed analogue system with a poorly installed high-definition (HD) camera system is unlikely to provide much benefit; the risk to the police of being swamped with useless data being just one negative outcome.

I look at the emerging world and recognise the scale of the work ahead. The National Surveillance Camera Strategy is a perfect vehicle to deliver against these challenges, but appropriate resources need to be unlocked to enable delivery.

The following represents a synopsis of the emerging issues distilled from the horizon-scanning report compiled by Neil Cohen.

## Surveillance Cameras Are No Longer Just Cameras…

Many of the issues that may raise public concerns in the future will be related not simply to the cameras themselves but to the advanced analytics technologies to which these cameras could be connected. Practically this suggests that there is a need for new standards and guidance to cover the operation and use of some of these technologies. Current standards such as BS EN 62676 are good at setting standards for and guiding the installation of traditional CCTV systems, but do not cover the use of more advanced

technologies such as automatic facial recognition and video analytics. They also do not address issues of cybersecurity, which are increasingly relevant as surveillance camera systems become part of larger data networks.

These are issues that were raised during the *Question Time* themed event (under the citizen engagement strand, see also Chapter 3) held at the London School of Economics in February 2018.

Some work is under way within international standards groups – for example, in the areas of video analytics and in biometrics, but these are at a relatively early stage. The challenge is to determine what features would be required from these standards to give the best assurance to the public that the technology is being deployed appropriately and effectively.

There are also some standards that cover specific deployments of surveillance cameras, for example, the recently published BS 8593 for the use of body worn video devices. However, it will be necessary to consider the development of further device-specific standards in future (unmanned aerial vehicles or drones). The horizon-scanning report makes the following recommendation.

> *"**Recommendation:** Develop specific guidance and standards to focus on those advanced technologies most likely to raise public concern when deployed in public spaces, for example, automatic facial recognition and video analytics. These should cover both performance and the appropriate use of the technology, and embed consideration of cybersecurity."*

## Who Has the Best Technology?

The internet giants are investing heavily in advanced video analytics technologies to search through online content. Some of this sophisticated technology is then made available to the public/consumer. The commercial retail sector also invests in advanced technologies to understand and target their customers. By contrast, most relevant authorities (as defined in the Protection of Freedoms Act 2012 (PoFA)) such as local authorities have aged CCTV systems, and limited budgets for investment in advanced and potentially intrusive technologies. Will this ageing infrastructure have an impact on how the deployment of novel video surveillance technologies is thus increasingly likely to occur first in a sector that is outside of my current statutory remit? The SC Code does, however, mandate the Surveillance Camera Commissioner to encourage non-relevant authorities to adopt the SC Code. The horizon-scanning report makes the following recommendation.

> *"**Recommendation:** Consider whether the restriction of the remit of the Surveillance Camera Commissioner to focus on relevant authorities is still appropriate for providing adequate oversight over the deployment of video surveillance technologies in public spaces."*

## Is That Really Possible?

The increasing use of advanced video surveillance technologies in public spaces, especially when coupled with high-resolution multi-megapixel cameras, is likely to affect the perceived (and real) level of intrusiveness of public space video surveillance. The general level of public support that currently exists for traditional CCTV may not be maintained in the face of widespread (and potentially inappropriate) deployment of advanced video surveillance technologies with much more intrusive capabilities.

Furthermore, as technologies develop in both complexity and in capability there is an increasing risk of misunderstandings in the public mind around the abilities and limitations of surveillance camera technology. The horizon-scanning report makes the following recommendations.

> *"**Recommendation:** Improved guidance for the public to help to provide a realistic understanding of the capabilities and limitations of advanced video surveillance technologies. Also guidance for the public wishing to deploy such technology.*
>
> ***Recommendation:** (Following on from above) Open public debate on the future use of advanced video surveillance technologies."*

I am pleased to say that under the civil engagement strand, the National Surveillance Camera Strategy is already addressing these observations. However, I do not believe that this will be a quick fix or easy to achieve. I am already seeing contrary reporting by interested parties around the efficacy of such issues as the performance measures applicable to automatic facial recognition technology. One side of the debate suggests that the technology is wholly inaccurate; another side argues that this reporting is utterly misleading and ignores context such as human intervention. I believe that a single narrative outlining the performance is essential to inform the public. I shall be championing that approach during the coming year.

## Where is my Data?

With the growing use of cameras within a broad range of devices such as smartphones, body worn video cameras, drones and vehicles (driverless vehicles in future), and the growing ability to network these devices and store images remotely, it may become increasingly difficult for a member of the public to identify:

- who operates a given camera;
- for what purpose; and
- where those data are stored.

A potential future example is a driverless car, where the camera footage is fed back to an insurance company, or to the fleet owner, or direct to the police in the case of an incident. The new DPA will provide greater reassurances and oversight. The horizon-scanning report makes the following recommendation.

> *"**Recommendation:** There may be a need to consider providing greater information at the 'front end' of a camera system, to inform the public about its deployment."*

## Clever Technology Will Not (Entirely) Replace the Need for Competent People

At some stage, perhaps via developments in AI, algorithms deployed in applications such as video analytics and face recognition may become demonstrably and routinely more reliable than a trained human operator undertaking the same task even in complex scenarios. This may have a range of implications including, for example, the processes through which evidence is gathered and assessed in police investigations.

However, in the meantime the deployment of novel technologies will not eliminate the requirement for the end-users of this technology to be competent, effective and well trained in its use.

Advanced technologies are also only effective if specified and installed correctly. The widespread use of new technologies will not by itself be a cure for failings in surveillance camera systems caused by poor installation and maintenance, or equipment that is not fit for its intended purpose. Additionally, the system owner needs to have the capability and capacity to act on the information provided by the video surveillance system. These problems are just as likely to exist in new systems as in old ones.

Therefore, the need will remain for standards and training, and this training will need to be updated to allow for the most effective installation and use of advanced technologies. The horizon-scanning report makes the following recommendations.

> *"**Recommendation:** Training courses to be developed to cover the practical installation and use of advanced video surveillance technologies such as automatic facial recognition and video analytics.*
>
> ***Recommendation:** Raise awareness and promote the take-up of standards, particularly during procurement exercises."*

## But Is It Useful?

The growing volume and range of sources of video surveillance data (plus all the other data to which they may be linked) may ultimately need to be shared with the criminal justice system (CJS) should it be required in the investigation of an incident. Equally, to prevent data overload, the guidance from the Information Commissioner's Office (ICO) to retain data for no longer than necessary should also be borne in mind. Trust in the data is also critical. How can this be retained given the increasing ability to manipulate imagery?

More generally, the lack of clear measures of effectiveness still constrains the debate around the value of video surveillance, particularly lack of measures of its effectiveness in the detection and investigation of crime. This in turn limits the ability of local authorities and law enforcement to make a case for continued investment in the technology, potentially further increasing the capability gap between what is available to relevant authorities and what is available to other sectors. The horizon-scanning report makes the following recommendations.

> *"**Recommendation:** System owners should consider the needs of the CJS and the means to interface with it as part of the system specification. Equally, policing and the courts continually need to upgrade their capability to recover, process and analyse increasingly large volumes of data.*
>
> ***Recommendation:** The CJS also needs to better demonstrate the value of the information to system owners and to those responsible for funding further investment. Work should be undertaken to strengthen the evidence base around the use of surveillance camera technology."*

## Political, Economic and Legal Considerations

The potential likely development and reach of surveillance technology is so complex and fast moving that it is difficult for politicians and senior policy makers to fully understand the implications. The state is probably powerless to stop consumer-driven technology from being used.

Is 'the state' the right target for regulation when there is much more powerful technology in private hands? I have repeatedly made recommendations for the Government to expand the focus of the SC Code. I have recently made what I consider to be a powerful argument for the NHS (not a relevant authority) to be included within the statutory remit of the SC Code as a relevant authority.

There is a question around the ownership of surveillance data in the future. Clearly the state has an obligation to protect its data but how will those data be accessed by other state operators for, say, other law enforcement purposes? Under which jurisdiction will the use of data fall?

'Fake news' – there is an increased risk (and perception) of images being manipulated. Can surveillance images be trusted – from either the Government or private sources? I see the role of defining standards becoming increasingly important if, for nothing else, to provide reassurance to the public that this vast surveillance infrastructure actually protects them, and does not threaten them.

## Ethical Considerations

The state has a duty to ensure that the surveillance images in its possession must be used within an ethical framework. Several examples were given of where surveillance technology had been used by authorities (both central government and local government) in an inappropriate manner (a well-known comedian being filmed by a police helicopter being just one such example). The following short list illustrates the point.

- Using video surveillance to spot people putting the wrong rubbish in their recycling bins and then levelling a charge.
- Widespread use of video surveillance in car parks, installed to stop vehicle crime but used to catch and fine over-stayers.
- Police images being uploaded to YouTube.

In the longer term, is a surveillance ethics committee needed as more sophisticated tools become available? Maybe a guiding principle should be that 'just because you can do it does not mean that you should do it'?

What ethical framework applies to non-state use of surveillance camera technology (or third-party data acquired from surveillance camera technology)? For example:

- the capture and sharing online of a video made by a member of the public on social media platforms;
- the capture and storage of surveillance camera data by the private and commercial sector for an increasing range of purposes, with increasingly sophisticated video analytics capabilities, linking various sources of data together (for example, automatic number plate recognition/face recognition/shopping habits).

What if the data or the conclusions derived from the data are incorrect? What are the consequences for an individual and how can you tell?

What about ethics of systems when the human is removed from the decision-making process? At some point the computer will (probably) be able to make a better decision than the human operator. Does a human need to be in the loop to make a positive ID on a suspect?

Is there sufficient understanding by the public or the Government about how the technology works or how it is used? Do they have a realistic understanding of the capabilities and limitations? Should they? There may be a role for the Surveillance Camera Commissioner in informing the public, to help to address some of the myths and misunderstandings. This will be necessary before we can have a proper debate.

# Chapter 3 – National Surveillance Camera Strategy for England and Wales – Civil Engagement

In devising this National Surveillance Camera Strategy I was conscious the Government's clearly stated intent that *"the purpose of the Code will be to ensure that individuals and wider communities have confidence that surveillance camera systems are deployed to protect and support them, rather than spy on them"* (paragraph 1.5, Secretary of State's Surveillance Camera [SC] Code of Practice).

Professor William Webster, Director of the Centre for Research into Information, Surveillance and Privacy (CRISP) and Professor of Public Policy and Management at the University of Stirling leads the civil engagement strand[19] of the strategy. Professor Webster's involvement in this approach has been crucial. At a time where new technologies are increasing exponentially, their capabilities are little understood by the public at large and their impact on society yet to be determined, the requirement to involve the public in any debate about their usage is seen as paramount.

The delivery plan for his strand was shaped to start the debate, and the engagement plan was placed on my GOV.UK website as promised.[20] Its stated aims are to ensure that:

- citizens have free access to information relating to the operation of surveillance cameras;
- citizens have a better understanding of their rights in relation to the operation of surveillance cameras;
- citizens have an understanding of how surveillance cameras function and are used; and
- organisations have an understanding of the information relating to the operation of surveillance cameras that they should make available to citizens.

I am delighted to report that in February 2018 Professor Webster and colleagues delivered on the *Question Time* themed event at London School of Economics. Chaired by Professor Pete Fussey (Director of CRISP), we were joined by a stellar panel including Mike Barton (Chief Constable of Durham Constabulary and National Police Chiefs' Council (NPCC) lead for crime operations), Silkie Carlo (Big Brother Watch), Simon Israel (Channel 4 Senior Home Affairs Correspondent) and Lord Brian Paddick (Liberal Democrat House of Lords spokesperson for Home Affairs).

The event was very well attended and provoked a lively and challenging debate across the panel and the audience, as well as an active debate on Twitter.

---

19 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704453/Strategy_plan_3_-_civil_engagement.pdf

20 https://www.gov.uk/government/publications/surveillance-camera-strategy-civil-engagement-plan

I was interested in the panel's views on an issue raised from the floor:

> *"Would the panel support an integrated network of surveillance cameras, between private and public ownership, across the UK – effectively providing a security network to the police and intelligence agencies?"*

It is safe to say that this vision for the future was not supported by the panel. Views expressed ranged from intrusive to dystopian and incompatible with a modern forward-looking nation. Again the issue of privacy versus security was central to the debate.

These are exactly the types of debate we need to see more of and provide to the public if the notion of 'surveillance by consent' is to retain any sort of legitimacy. The debate has been published online.[21]

To complement the in-depth approach to public consultation delivered by the *Question Time* themed event I am looking forward to delivering the 'Surveillance Camera Day', which is currently scheduled for 2019. The aim is to encourage organisations to explain their use of such equipment and encourage more transparency in their operation. It is also clearly focused on attracting national media attention on the issues and further enable informed debate to take place at all levels of society.

In the coming year I am looking for further opportunities to 'continue the debate'. Historically many within the video surveillance camera industry have fallen back on the overwhelming public support for video surveillance. Video surveillance is a somewhat anachronistic term for what is being deployed on the streets of the UK. Those cameras might look like mere CCTV cameras, but have capabilities that stretch far beyond the mere image capture. The previous chapter on horizon scanning within the strategy more than eloquently lays out the reality of their use. The public need a say, they need a voice and I am determined to provide that. To that end Professor Webster and his colleagues at CRISP will be considering the possibility of more public-facing events in the reporting year.

---

[21] https://www.stir.ac.uk/about/faculties-and-services/stirling-management-school/our-research/research-areas/management-work-and-organisation/current-projects/

# Chapter 4 – National Surveillance Camera Strategy for England and Wales – Policing

Of all the relevant authorities described within Section 33(5) of the Protection of Freedoms Act 2012 (PoFA) it is arguably the Chief Officers of the police who most evoke public sensitivities in respect of the surveillance camera systems they operate. It is the police after all that are charged with the responsibility of keeping communities safe from ever evolving threats. It is reasonable therefore to expect the police to explore and harness the potential within surveillance technologies in that regard, and to use them to keep us safe from serious threats. However, surveillance technologies should only be used in justifiable circumstances where their use is lawful, ethical, proportionate and transparent. In equal measure the public also need to be safe from disproportionate and illegitimate state intrusion, and must have confidence that those technologies being used have integrity.

It was largely for those reasons that I determined that the police should be a key strand of work within the framework of the National Surveillance Camera Strategy[22] as follows.

> *"Objective 4 – The police proactively share relevant information about their own operation of surveillance camera systems and use of data."*

I have received support in that regard by the lead officers representing the National Police Chiefs' Council (NPCC) lead for CCTV, particularly from their support staff. To date, however, most of the work that has been conducted in progressing the deliverables that underpin this strategic area has largely been progressed by my offices, with occasional support from the NPCC and its offices. I would like to see this dynamic reversed going forwards.

In his 2016 Annual Report – *The State of Policing*[23] – Her Majesty's Chief Inspector of Constabulary Sir Tom Winsor made the following observations.

> *"The police are particularly far behind many other organisations in the way they use technology. There are good examples of forces using innovative technology or making innovative use of existing technology, but these are too few and far between … For too long, a culture of insularity, isolationism and protectionism has prevented Chief Officers from making effective use of the technology available to them. This needs to change."*

Given those observations, in the context of surveillance camera systems the seemingly increasing appetite of police forces to harness technology in connection with surveillance camera use is understandable. However, it remains incumbent upon them to demonstrate that they are operating ethically and in accordance with the laws that govern such use, specifically section 33(1) PoFA and the Secretary of State's Surveillance Camera (SC) Code of Practice, the Regulation of Investigatory Powers Act 2000 and the Data Protection Act 2018 (DPA).

---

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704456/Strategy_plan_4_-__policing.pdf

[23] https://www.justiceinspectorates.gov.uk/hmicfrs/publications/state-of-policing-the-annual-assessment-of-policing-in-england-and-wales-2016/

## The Protection of Freedoms Act 2012

Regulators have a key role to play in providing guidance where necessary and to hold the police to account in appropriate circumstances. The PoFA places a statutory responsibility upon the Chief Officers of police forces in England and Wales to have regard to the SC Code in respect of the surveillance camera systems that they overtly operate in public places. Those statutory responsibilities are not new and indeed have endured for five years.

Since 2000 the Information Commissioner's Office (ICO) has issued its own code of practice currently titled *In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information*. The ICO also publishes guidance relating to surveillance camera systems such as drones, and engages in public-facing media regarding surveillance camera system use in the context of the DPA. Of course, the ICO has a far wider geographic and contextual remit than I. I find ICO guidance to be good and recommend it to system operators and the public alike. However, with two very similar codes in existence that target operators of surveillance camera systems I continue to harbour concerns about the potential for the police to confuse their responsibilities arising from the SC Code with data protection responsibilities, even though both codes signpost each other. Indeed the *Post-Legislative Scrutiny of the Protection of Freedoms Act 2012* presented to the Home Affairs Select Committee commented:

> *"There has been some confusion regarding the role of the Surveillance Camera Commissioner and the ICO."*

And:

> *"There is an overlap in the roles, given that the ICO already oversees the privacy aspect of surveillance camera systems and can take enforcement action under the DPA for any breaches."*

## Assessment of Police Compliance with Section 33(1) PoFA and the SC Code

It was within this context therefore that I conducted an assessment as to the nature and extent to which police forces in England and Wales were operating surveillance camera systems regulated by the PoFA and also the extent to which they complied with their statutory responsibilities arising from section 33(1) PoFA.

In terms of methodology, in August 2017 I wrote to the Chief Officers of the 43 regional police forces in England and Wales and also the British Transport Police and the Civil Nuclear Constabulary. In doing so I asked Chief Officers to complete a simple survey document to:

- account for the surveillance camera systems that their force operated overtly as described at section 29(6) PoFA; and
- disclose whether they complied with section 33(1) PoFA in respect of each system operated, and explain how that compliance was demonstrated.

The surveillance camera systems operated by police forces in England and Wales that typically fall within my remit are CCTV, automatic number plate recognition (ANPR), body worn video cameras (BWVs), unmanned aerial vehicles (UAVs), helicopter borne cameras and indeed other systems such as dashboard mounted cameras. Emerging technologies

such as facial recognition systems are also specifically included within the SC Code. I therefore invited Chief Officers to be specific in their responses for each category of system.

Chief Officers were also invited to report as to whether or not they had appointed a senior responsible officer (SRO) with corporate responsibility for ensuring PoFA compliance in respect of the relevant overt surveillance camera systems that their force operated. The appointment of an SRO is not a requirement of the PoFA or indeed a requirement of the SC Code. It is simply a matter of good practice that I have recommended; such an approach mirrors the good practice identified in the context of covert surveillance at paragraph 3.29 *Home Office Code of Practice for Covert Surveillance and Property Interference*, issued under the auspices of the Regulation of Investigatory Powers Act 2000.[24]

I invited Chief Officers to respond to my offices by 30 September 2017 so that the results could be assessed. The process was undertaken in consultation with the Association of Police and Crime Commissioners and the NPCC lead for CCTV, who represents the NPCC on both my Advisory Council and the National Surveillance Camera Strategy forum. I am grateful to those bodies for the support that they provided.

## Survey Findings

I was delighted to note that all 45 Chief Officers responded so fully to the demands I made of them, and I commend their commitment in that regard.

It is important to emphasise that the results of this survey simply amounted to being a 'snapshot' of the use of surveillance camera systems as defined by the PoFA by those police forces surveyed in England and Wales between 2 August 2017 and 30 September 2017. The survey findings are purely based upon the information reported by the police to my offices and were not additionally or independently verified further.

As a regulator I have no powers of sanction or of enforcement, nor do I seek any. My role is to recommend, encourage and advise. In that regard therefore I have not sought to identify individual police forces within my survey findings. I hope that by adopting such an approach, Chief Officers are encouraged to consider their original responses to me in the light of subsequent recommendations I have made. These aim to ensure that their overt surveillance camera systems in public places accord with the law that I regulate.

To assess if forces are complying with the PoFA the survey asked for the following information.

- Has a self-assessment document as provided by the Surveillance Camera Commissioner been completed in respect of this system? If 'no' please provide the rationale together with an explanation as to any future intentions in that regard.
- If your force demonstrates regard to the SC Code other than by means of self-assessment, please provide details as to how this is addressed.

If forces responded that they had not completed the self-assessment tool or were unable to show how they complied by other means, this has been interpreted as not being able to demonstrate compliance with the PoFA.

---

[24] https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Key headlines arising from the submissions received were as follows:

- **Senior responsible officer** – although not a requirement of the PoFA, 32 (71%) of the 45 police forces in England and Wales participating in the survey reported that they had appointed an SRO with responsibility for PoFA compliance and 13 (29%) had not. I do not know whether the appointment of the SRO was made before, or as a result of my survey process being received by forces, I am, however, encouraged by the response.
- **Relevant surveillance camera systems** – 5 police forces (11%) reported compliance with section 33(1) PoFA in respect of all the relevant surveillance camera systems operated by them. Conversely 8 forces (18%) reported compliance in respect of only 1 system amongst those they operated, and 2 forces (4%) did not comply in respect of any of the systems that they operated.
- **CCTV** – 40 police forces (89%) reported that they operated CCTV systems; 27 of those (68%) reported that they operated internal CCTV systems monitoring public 'help desk' areas, of which 9 (33%) were reported as being compliant with section 33(1) PoFA. There was an inconsistency of understanding as to what systems were relevant to this section of reporting; in some instances references were made regarding the use of CCTV systems operated by local authorities, and differing arrangements that existed.
- **Automatic number plate recognition** – 44 police forces (98%) reported operating ANPR systems; 5 police forces (11%) indicated that the ANPR systems that they operated were not compliant with the PoFA. Reasons offered for this included a lack of awareness of the legislation.
- **Body worn video cameras** – 42 of the 45 police forces (93%) confirmed that they issued BWVs to their staff either as a stand-alone force arrangement or as part of a regional collaboration with other forces. Of these 14 forces (33%) indicated that they did not comply with the PoFA, while 2 forces – the Greater Manchester Police and the Metropolitan Police Service – have attained my certification mark for their BWVs. The remaining 3 forces (7%) reported that they did not use BWVs.
- **Unmanned aerial vehicles/drones** – 25 of the 45 police forces (56%) responding to this category in the survey reported that they had a UAV capability; 14 of those forces (56%) reported compliance with the PoFA. Three forces – Devon and Cornwall (jointly) and Dorset – have attained my certification mark for their use of UAVs.
- **Helicopter borne cameras** – the National Police Air Service (NPAS) complies with the PoFA in respect of the systems it operates.
- **Other systems** – there was an inconsistency demonstrated by police forces when responding to this section of the survey, as to what other systems should actually be reported upon. Examples variously reported included dashboard cameras, helmet cameras and evidence gathering activities using video recorders.

It was curious that amongst reasons cited for not complying with the PoFA, where one was volunteered, was a lack of awareness of the legislation and of the SC Code – respondents were asked to respond on behalf of their force. This is something that the NPCC should consider further in terms of what it can meaningfully do to raise awareness within police forces as to these issues.

## Recommendations

Having assessed the outcome of the responses submitted to my offices I made two recommendations that were specific to Chief Officers and in connection with which I invited them to respond. My recommendations were as follows:

- It is recommended that all police forces in England and Wales identify a senior responsible officer (SRO) who has strategic responsibility for the integrity and efficacy of the processes in place within the relevant authority to ensure compliance with section 33(1) PoFA and of those processes and responsibilities associated with the implications of sections 33(2), 33(3) and 33(4) of that Act.
- It is recommended that police forces conduct a review of all surveillance camera systems operated by them to establish whether or not those systems fall within the remit of section 29(6) PoFA. The advice of force legal advisors may be required in some circumstances. Where systems are so identified there should be processes in place that enable the police to discharge their responsibilities effectively under the PoFA in respect of those systems. Such processes should also keep the development, procurement and operation of future systems under review so as to appropriately determine and address the inherent legal responsibilities associated with their operation. The force SRO should lead this work.

Additionally, I made a third recommendation to be considered by the NPCC.

- It is recommended that the National Police Chiefs' Council (NPCC) representative for CCTV considers the workstream being conducted under the umbrella of the National Surveillance Camera Strategy to deliver a national service level agreement framework for CCTV between the police and local authorities with a view to providing support to its delivery.

In making my recommendations to Chief Officers I also wrote to the Ministry of Defence Police and the National Crime Agency, both of which are also 'relevant authorities' under the PoFA.

So as to share good practice, I additionally wrote to the Chief Officers of Mersey Tunnels Police, the Port of Bristol Police, Port of Liverpool Police, Port of Dover Police, Port of Felixstowe Port Police Unit and the Port of Tilbury Police.

## The Police Response

Whereas I was concerned with the headline responses in the first instance I was particularly reassured by the responses I subsequently received from Chief Officers to the recommendations I had made. Every Chief Officer without exception responded positively and accepted both recommendations I had made. Taking Chief Officers at their word as I do, all relevant police forces should now have:

- an SRO appointed and clearly identifiable within each force with corporate responsibility for PoFA compliance; and
- systems in place to assess and deliver compliance with the SC Code in respect of the surveillance camera systems that they operate in public places, now and in the future.

The requirements of section 33(1) PoFA and the SC Code form part of a legal framework that governs the police use of surveillance cameras. Where images or other evidence are to be adduced in judicial proceedings and have been captured by a surveillance camera system being operated by a relevant authority, a failure to comply with these provisions should be revealed to the Crown Prosecution Service (CPS) prosecutor so that a disclosure test may be applied. I am grateful to the CPS for its efforts in reminding its prosecutors to test these matters when dealing with police prosecution files in appropriate circumstances, and committing to update their Disclosure Manual.

Given the rapidly changing capabilities of surveillance technologies and the increasing complexities of public and private partnership (between police and retail/business and others) I will be calling upon the NPCC to redouble its efforts in supporting the strategy. Too often do I hear complaints from local authorities that there is insufficient strategic engagement from police forces, too little feedback on imagery and data exchange. We have benefitted from extremely supportive senior police engagement in the past but, at the same time, suffered from a quick throughput of those officers and too little continuity. Public space surveillance is a huge industry and needs to be treated as a strategic asset to law enforcement. I shall be engaging with the NPCC to raise my concerns and seek its support in the provision of a video surveillance lead with some longevity.

As surveillance camera technologies continue to evolve, as they surely will, and the police use of those technologies proliferates, as it undoubtedly will, so will the imperative for the police to demonstrate transparently that they operate in accordance with the law in proportionate and justifiable circumstances. These are fundamental considerations of public trust and confidence. In that regard I very much look forward to a re-energised and active engagement with the NPCC once a new lead officer for CCTV is appointed.

## Conclusions Drawn from the Survey

It is understandable that the prospect of the police and law enforcement agencies seeking operational recourse to increasingly advanced surveillance technologies breeds a sense of disquiet in some quarters. Indeed these are matters that continue to occupy and significantly challenge my thoughts.

Whatever views exist, regulatory or otherwise, it is inescapable that the threats to our society are evolving in terms of complexity, technological capability and volume. Those threats are increasingly challenging to the finite resources of our police and law enforcement agencies working in a digital age. To deny the police the opportunity to exploit technologies to keep us safe, technologies that are in everyday use elsewhere for our convenience, and to scaremonger in a manner that inappropriately and adversely impacts upon the ability of the public to have a balanced view on such matters, is to risk constraining our police to an analogue law enforcement capability. The challenge for the police using surveillance camera technologies is to engage and keep the public informed, whilst working ethically and in accordance with both the letter and the spirit of the law. Lawmakers and regulators need to ensure that a framework of legitimacy, integrity and regulation properly guides, harnesses and effectively holds the police to account. Therein lies my mission.

## Automatic Number Plate Recognition

The use of this technology by the police continues to occupy a good deal of my time. In previous reports I have focused on the sheer size and scale of its use by law enforcement in the UK.

Last year I reported that the daily capture of between 25 and 40 million reads of vehicle registration numbers by around 9,000 cameras (and increasing) and the subsequent storage of 20 billion read records is formidable. The length of time for data storage, of a maximum of two years, with safeguards upon its use, is more than anywhere else in Europe. During the reporting year I am delighted to say that the police and the Home Office have listened to my voice and that of others and commenced the reduction of data retention to 12 months. This is in line with the retention period for communications data.

Throughout my commission I have challenged the police and the Home Office on three fronts concerning the use of ANPR (these challenges can be found in annual reports 2015/2016 and 2016/2017):

- to what extent ANPR is being used lawfully in England and Wales (in relation to privacy, retention and proportionality);
- the transparency of its use; and
- the governance framework underpinning its use.

The undoubted value to policing of ANPR and the harnessing of new and emerging technology cannot be overlooked when making these challenges. However, maintaining public confidence and trust in its use is a key factor if the police are to maximise the value of such technology. Having made those challenges I have seen a police response that is extremely encouraging. In 2015 I proposed the establishment of an independent advisory group to provide an opportunity for high-level engagement between the police and the Home Office with experts, specialists in the field, lawyers and civil liberty groups. This group should operate as a critical friend to the police and challenge openly and transparently.

I was delighted to be approached by the NPCC lead, Chief Constable Charlie Hall, and asked to chair the national Independent Advisory Group (IAG) on ANPR. The terms of reference and minutes of meetings are posted on my website.[25] Again I must offer my thanks to the extremely talented members of the group who range from lawyers, civil liberty groups, the police, local authorities, police and crime commissioners, motoring organisations, fellow regulators and more. This group provides oversight on behalf of the citizen and gives an opportunity to focus on both strategic issues and tactical usage. I will not rehearse the outcomes of the initial IAGs but the reader will see that the group is already focusing on data, standards, performance and accountability, and has a clear feedback loop direct to the NPCC lead.

Greater transparency in terms of the use and governance of ANPR has also been addressed and the NPCC website is seeking to provide much more information, data and insights as to its governance, how policy and standards are set, and so on.[26]

However, there remains much to do. ANPR currently operates under a complex framework of legislation of general application (common law, the Data Protection Act 2018, the Human Rights Act 1998, the PoFA) and policy documentation, but without a single statutory provision. Its use is expanding from its initial focus of providing intelligence on serious and organised crime and national security issues, to supporting the collection of revenue from vehicle excise duties and motor insurance offences. There remains limited democratic oversight for such a powerful tool in the policing armoury.

---

[25] https://www.gov.uk/government/publications/automatic-number-plate-recognition-advisory-group-terms-of-reference
[26] http://www.npcc.police.uk/FreedomofInformation/ANPR.aspx

I repeat my calls for ANPR to be placed on a clearly defined statutory footing through the introduction of a single legislative provision at the first available opportunity. Readers of my previous reports will be aware of my views on data retention and evidencing the value of ANPR. The public have, as an absolute minimum, the right to know and understand how the data are used, their quality and their accuracy. My IAG provides the advice that legal risks remain due to the lack of an evidence base regarding the use and value of ANPR data. Indeed a comprehensive list of requirements has been formulated by the IAG and submitted to Chief Constable Hall.

Principle 3 of the SC Code provides guidance to system operators and controllers concerning transparency in the use of surveillance cameras. Much more can be done to follow that guidance and 'demonstrate due regard' to the SC Code.

I recommend the introduction of comprehensive audit capabilities within the National ANPR Service (NAS):

- to mandate compliance with the National ANPR Standards for Policing (NASP); and
- provide a centralised dataset from which an evidence base of ANPR use could be drawn.

Effectively ANPR is an emerging national system with its roots at the local constabulary level. Much more needs to be done to provide clarity as to the value of this system.

I continue to urge the NPCC to develop a national communications plan that will provide some much needed information to the public concerning its use, value and capability.

I firmly believe that, given the passing of the PoFA and the introduction of the role of the Surveillance Camera Commissioner (SCC), there is a persuasive argument to designate responsibility for oversight of ANPR to a single body. Currently that function sits between the ICO and SCC. The role of the Investigatory Powers Commissioner's Office (IPCO) is, in my opinion, stand alone and its role and remit is clear and supportive of good oversight. Similar arguments are to be made in relation to the emerging use of facial recognition technology via surveillance systems.

## The National ANPR Service Programme

The delivery of NAS as the replacement of the National ANPR Data Centre (NADC) will provide a new framework under which ANPR data are collected, processed and retained. I believe that the NAS programme – and the eventual service itself – ought to address many of the issues that I have identified through the IAG. However, I am determined to maintain an oversight on its development; given the absence of a statutory footing it is important that I maintain that regulatory focus.

I recommend that a dedicated, independent policy function is mandated with the NAS programme to ensure that ANPR policy, and compliance implications of programme decisions related to data management, transaction logging, audit functionality and other areas are adequately considered. I am concerned, at the time of writing, that the funding for a police national co-ordination role in respect of ANPR has ceased.

## ANPR Data Quality

I have stated frequently that law enforcement use of ANPR in the UK must surely be one of the largest data gatherers of its citizens in the world. The daily capture of around 50 million reads of vehicle registration numbers by around 9,000 cameras and the annual storage of 20 billion read records is formidable.

The use of ANPR has grown beyond the fight against serious crime. It is now used by those outside of law enforcement to manage traffic flows, control speeding, and for prosecutions for non-payment of vehicle excise duty, where other options have been unsuccessful in achieving compliance.

My focus on ANPR data quality has emerged from guiding principle 12 of the SC Code:

> *"Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date."*

In my previous Annual Report I expanded upon the issues of data quality, misreads and the impact of misreads from a police operational perspective, as well as how this can affect individuals whose plates have been misread. I will not rehearse those arguments here but will refer the reader to that report.

However, in conjunction with this issue I also focused on the quality of number plates and quality of camera (type approval). I referenced that ANPR depends on the quality of number plates it captures and stated:

> *"… the whole infrastructure is predicated against the fact that number plates do what it says on the plate – allow you to read the number."*

I have been providing detailed technical advice during discussions with the Driver and Vehicle Standards Agency to agree the new wording for the MoT guidance for testers. The aim is to ensure that number plates could in future be failed if they exhibited features that would make them difficult for an ANPR system to read accurately.

## Automatic Facial Recognition

In last year's Annual Report I highlighted the potential impact of new and emerging technologies, such as automatic facial recognition (AFR) technology, and stated the following:

> *"The advent of integrated surveillance technologies (cameras, sensors, analytics, biometrics, smart systems) means that the ability of the state and indeed the commercial sector to physically and intrusively track the citizen in public spaces is well and truly upon us and may in future, point to the requirement ... for an overarching style of regulation of open source surveillance."*

Further I commented:

> *"Integrated surveillance camera systems can provide new ways of protecting citizens in a world where concerns about terrorist atrocities are sadly becoming more prevalent. Greater debate around the capabilities and integration of those systems and their operation by both public and private sectors need to be held. The public need to have confidence that operators of these systems can be trusted to use them lawfully, proportionately, ethically and only where their use is legitimately needed."*

We now see Big Brother Watch and Liberty raising litigation against the Metropolitan Police and the South Wales Police respectively for their use of such technology. We have also, at last, seen the release of the Home Office Biometrics Strategy that was long overdue. This strategy, whilst not providing a clear road map providing clarity and direction, does at least provide a foundation for that work to be commenced.

Throughout the year I have been endeavouring to energise engagement, discussion and debate on this matter with, amongst others, the Home Office, government ministers, the NPCC, police forces, civil libertarians, the public and indeed fellow regulators. It is a matter that is gathering momentum in the public consciousness and I will continue to encourage debate and engagement, as I believe that doing so will be a catalyst for change in support of the public interest. The public interest demands clear legislation, transparency in governance and approach and a coherent and effective regulatory framework in which they can have confidence.

It is asked – should the police even consider using such technology in the first place? Consider the view of the eminent Lord David Anderson KBE QC, formerly the Government's independent reviewer of counter terrorism legislation who said:

> *"… either you think technology has presented us with strong powers that the government should use with equally strong safeguards or you believe this technology is so scary we should pretend it's not there. And I firmly believe in the first category not because I say government is to be trusted but instead because in a mature democracy such as this one we're capable of constructing safeguards that are good enough for the benefits to outweigh the disadvantages."*[27]

The SC Code contains a number of provisions that are of specific relevance to the use of AFR and other technologies integrated with the operation of a surveillance camera system. In particular these include the following references:

> *"Para 2.1 'Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need …*
>
> *Para 2.3 'That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential now and in the future …*

---

[27] https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you/

*Para 3.2.3 'any use of facial recognition or other biometric characteristic recognition systems need to be clearly justified and proportionate in meeting the stated purpose and be suitably validated …*

*Footnote 4 'The Surveillance Camera Commissioner will be a source of advice on validation of such system' In this context the term validation means that the surveillance camera system being operated by a relevant authority is being operated in accordance with section 33(1) of the Act and in a manner which is consistent with the provisions of the SC Code …*

*Para 4.12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.*

*Para 4.12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology."*

You may be forgiven for asking why AFR is considered as a video surveillance system at all, when it is in fact merely a biometric algorithm. The answer lies in section 29(6) PoFA, which defines the surveillance camera systems of my focus as being:

- CCTV;
- ANPR;
- any other system for recording or viewing visual images for surveillance purposes;
- any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- any other systems associated with, or otherwise connected with those systems.

Two police forces have been engaged on pilots to assess the value and utility of AFR.

The Metropolitan Police Service (MPS) made use of AFR at the Notting Hill Carnival in 2016. This attracted concerns because the results of the deployment were not published, and concerns were raised regarding:

- the engagement, legality and reliability of equipment being used;
- the image database; and
- evaluation and governance.

The MPS repeated this exercise in 2017 and whilst concerns remained, the MPS reached out to regulators for guidance and completed my self-assessment tool and a Data Protection Impact Assessment (DPIA) issued by the ICO.

South Wales Police employs AFR and have used it at major sporting events. It has worked hard to engage stakeholders, the Home Office, regulators and the public and has ensured strategic governance and independent consultation.

Let me make it clear, I think that the police are genuinely doing their best with AFR in what I consider to be a complex legal and regulatory framework. It is inescapable that AFR capabilities can be an aid to public safety, particularly from terrorist threats in crowded

or highly populated places. It is inevitable therefore that there is an appetite, particularly within law enforcement, to exploit these capabilities; an appetite that is doubtlessly born out of a sense of duty and determination to keep us safe. Many of those technologies such as AFR already exist in society for our convenience. Therefore, the public will have something of an expectation that those technologies are so used by agents of the state, but only in circumstances that are lawful, ethical, proportionate and transparent.

By the same measure the public also need to be safe from disproportionate and illegitimate state intrusion. The challenge is arriving at a balance and for that to happen there needs to be a clear framework of legitimacy and transparency, which guides the state, holds it to account where necessary and delivers confidence and security amongst the public.

Unlike ANPR, there are no national standards in place regarding AFR and central co-ordination within the NPCC is still evolving. The Home Office has at last delivered a Biometrics Strategy but there is much work to do. The state is in the foothills of persuading the public that there is a sufficiently robust regulatory regime in place to provide public reassurance.

So what have I been doing about this issue?

- I have written to the NPCC lead for CCTV, ACC Tim Jacques, urging better strategic governance and suggesting that the College of Policing help to design standards.
- I have written to all Chief Officers in England and Wales reminding them of their responsibilities and my role under the PoFA.
- I have written to the Chair of the NPCC and to the Minister of Policing setting out my observations.
- I have met with other regulators and discussed areas of potential synergy.
- I have visited police trials on AFR in South Wales andthe Metropolitan Police.
- I have presented at numerous forums including the Police and Ethics Board in London and engaged with Her Majesty's Inspectorate of Constabulary (HMIC) and the CPS.
- I have even held a public engagement *Question Time* styled event at the London School of Economics to engage public opinion and debate with a panel of experts from across the civil spectrum (details in the citizens engagement strand in Chapter 3). In that regard, there is more to come.

Is the current and anticipated regulatory framework fit for the purpose of regulating technologically advanced surveillance camera systems in public? Well let us look at our regulatory fingers in the surveillance camera pie!

Firstly, the ICO – AFR relies on cameras and produces data – the ICO has a very clear strategic role in regulating the management and privacy of personal data – the General Data Protection Regulation (GDPR) and the new Data Protection Act 2018 (DPA) have now been enacted. The ICO is developing excellent guidance to help with what is an increasingly complex framework. It is only part of the regulatory picture however. The DPA protects against the misuse of private data but does not provide a legal basis for the conduct of such surveillance.

The Biometrics Commissioner – one senses this title must have some responsibility within this field. It makes good sense as the current Commissioner is the leading regulatory ambassador for ethical standards in the use of biometric capabilities. However, in the statute the Commissioner currently has no mandate where AFR is concerned. The Commissioner has been and continues to be a strong advocate for a more ethical approach to the use of custody images, and has made repeated calls for the production of a government biometrics strategy.

The Forensic Science Regulator very clearly sets and regulates the standards of digital forensics. These ensure that the public interest is appropriately served by standards of evidential and procedural integrity in cases where judicial proceedings involve the use of digital images.

The IPCO works in the field of data capture across a wide spectrum of covert techniques. Now in the covert domain the regulatory regime for covert surveillance is clear and unequivocal, and in my view reassuring.

There is a clear basis in law for covert surveillance to be conducted, provided by the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016. There are provisions for:

- independent judicial oversight and approval;
- a clear regulatory framework within the relevant legislation, which prescribes governance in so far as authorisation levels for covert surveillance activity is concerned;
- the key principles to be considered and recorded within specified timescales to ensure constant review; and
- an inspection regime, which scrutinises compliance in respect of every public authority that has powers vested in it to conduct covert surveillance, and which results in reports and recommendations being considered by senior officers and judicial figures alike.

That is a regime that has stood the test of time – 17 years – and is necessary because of the degree of intrusion that covert surveillance causes, and the use of technologies involved.

But arguably, overt surveillance is becoming increasingly intrusive on the privacy of citizens; in some cases more so than aspects of covert surveillance because of the evolving capabilities of emerging technologies. It may be AFR today but what about augmented reality, gait analysis, behavioural analysis, lip-reading technology and whatever else may be around the corner?

Technology can enable overt surveillance camera systems to harvest an exceptionally detailed picture of your private and personal information, in some cases far better than a surveillance officer covertly following you to the supermarket. My point is this – there is a clear legal and regulatory framework to underpin covert surveillance. There is a more complex legal framework that underpins overt surveillance activity, which includes common law, the DPA, the PoFA, the Freedom of Information Act 2000, the Counter Terrorism Act 2008.

Whereas the new GDPR and DPA provisions and proposals will undoubtedly provide a more comprehensive basis in law for the management of personal data, overt surveillance is a wider legal consideration of which the GDPR and DPA are elements, but not the all.

## A New Paradigm

I made it clear in my Annual Report last year that I believe the current regulatory framework needs to evolve to manage the challenges emerging from new surveillance technologies in society. My role has drawn me through the camera lenses and into the back office of artificial intelligence systems in the preceding five years.

I do think that the regulators can work closer together on these matters in bringing the debate to deliver tangible outcomes to benefit the public interest. Threats to society and threats to civil liberties are of equal magnitude these days, and are becoming increasingly complex. It is simply not satisfactory to expect law enforcement, emergency agencies and the public to 'just get on with it'. In the context of surveillance in society, voices who shout 'you should' or 'you shouldn't' resonate with equal conviction.

My view has consistently been that to establish a true balance regulators need to work closer together and the Government needs to engage far better than has hitherto been the case. Most importantly there needs to be a constant heartbeat of constructive and mature challenge and debate from the citizens of this country, who are ultimately on the other end of the camera lenses and its intrusive capabilities. The public voice is the lifeblood of change and progress to the greater good. We need to listen, to understand and to act sensibly and 'we' includes the Government.

# Chapter 5 – National Surveillance Camera Strategy for England and Wales – Local Authorities

Local authorities provide the backbone of service provision of video surveillance systems in society. The existence of CCTV operation rooms (as they are still known) is the legacy of the explosion in the use of such cameras in the 1990s. In previous annual reports I have focused on the impacts of austerity and ageing technology on such service provision, so I will not rehearse those points in detail here. Some commentators would have argued that such service provision is no longer required as the imagery is poor, evidence is therefore second rate, and local authorities arguably have better things to spend their money on.

However, police resources are stretched and there is still a need for these systems, whether to monitor behaviour in a vibrant night-time economy or search for a missing child or vulnerable person. CCTV is usually the first point of contact for the police, door staff or store detectives when assistance is needed. Indeed, some local authorities have embraced the use of CCTV to improve efficiency by promoting its use across departments to address issues from recovering costs for replacing street furniture damaged following road traffic collisions, which the local authority would otherwise have to pay for, to diverting public transport to avoid congestion.

Ironically these arguments have been overtaken by:

- the impact of advancing technology;
- the potential uses for artificial intelligence within smart cities; and
- linkages between video surveillance systems and sensor technology.

Local authorities and city leaders need to consider new paradigms that harness such technology, yet provide reassurance to the citizen that they are not descending into a dystopian era of surveillance suppression.

These considerations are actively under way in some quarters and my office is engaged where appropriate. The essence of work within the National Surveillance Camera Strategy[28] has focused upon driving up standards across the local authority network in relation to:

- certification;
- formulating a service level agreement (SLA) between local authorities and the police; and
- defining a simple suite of key performance indicators against which the value of such technology can be effectively measured.

Tony Gleason (CCTV Manager at Bournemouth Borough Council) has been leading the local authorities strand of the strategy, of which the SLA is a deliverable. Working alongside the policing strand we hope to have a framework SLA template document

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704472/Strategy_plan_5-_local_authorities.pdf

published within the reporting year. I had hoped that work on this important guidance would have progressed more quickly. However, at the time of writing there is currently no lead at the National Police Chiefs' Council (NPCC) for CCTV to help to drive this work forwards – this is disappointing.

Local authorities rely on information from the police on which they can evaluate the performance of their video surveillance systems. This in turn demonstrates the value of surveillance systems to chief executives and councillors in these austere times. I still hear complaints regularly from local authority CCTV managers that in some areas this information is not easy to obtain. A CCTV Manager survey by the Public CCTV Managers Association (PCMA) in 2017 showed that only 22% of police forces provided regular feedback to local authorities and 19% of local authorities had a dedicated police liaison officer. There needs to be senior police engagement to drive the work on the SLA forward and gain support across forces – developing and issuing the SLA is a priority for the reporting year.

A key focus has been to mirror our success with the police and identify a single point of contact across each local authority. This person will ensure that they can demonstrate that each video surveillance system is operating in accord with the Protection of Freedoms Act 2012 (PoFA) and key relevant legislation. To that end I have chaired a series of workshops across England and Wales identifying this requirement. I am delighted that Liverpool City Watch has shown leadership in this regard. It is working with the PCMA to develop a guidance document to reflect its success in driving through this important piece of work.

Whilst in the public mind it is the 'town centre' CCTV operations room that attracts the focus, time has moved on. Local authorities are deploying body worn video cameras, drone technology, automatic number plate recognition (ANPR) and, I expect, other forms of surveillance driven by artificial intelligence technology. These systems inevitably operate under different departments within an organisation, and standards of use, deployment and data management will vary. It is essential for public trust that these are operated to the same high standards as the larger operations rooms discussed earlier.

In 2015 I wrote to all local authority chief executives asking them to complete my self-assessment tool in respect of their main town centre scheme – approximately 95% of authorities completed the tool. In this reporting year I will be writing to local authorities again to gain an understanding of the totality of the video surveillance cameras they are operating to understand the level of compliance with the PoFA by those who must comply. In the same way that these organisation have a senior responsible officer (SRO) for covert surveillance and a data protection officer (DPO), I will be asking for a SRO for public space video surveillance cameras. This could well be the covert surveillance SRO or the DPO. I will work with those identified people to help to drive up standards across local authorities.

In terms of standards, my third-party certification mark continues to be something local authorities seek to attain with 38 authorities having been awarded the mark at the time of writing. There is still a lot more to do here and I will be working with the three certification bodies,[29] the PCMA and others to encourage local authorities that want the mark to get it.

[29] IQ Verify, the National Security Inspectorate and the Security Systems and Alarms Inspection Board (SSAIB).

# Chapter 6 – National Surveillance Camera Strategy for England and Wales – Voluntary Adopters

The Secretary of State's Surveillance Camera (SC) Code of Practice, and the supporting National Surveillance Camera Strategy[30], provides a holistic 'whole system' approach for the management of video surveillance systems. I continue to focus on all organisations using such equipment in the public domain because the Protection of Freedoms Act 2012 (PoFA) and the SC Code place a burden of responsibility to encourage voluntary compliance amongst those sectors.

Paragraph 1.8 of the SC Code states:

> *"However, the government fully recognises that many surveillance camera systems within public places are operated by the private sector, by the third sector or by other public authorities (for example, shops and shopping centres, sports grounds and other sports venues, schools, transport systems and hospitals). Informed by advice from the Surveillance Camera Commissioner, the government will keep the Code under review and may in due course consider adding others to the list of relevant authorities pursuant to section 33(5)(K) of the 2012 Act [PoFA]."*

Indeed, at the outset of my commission, I recognised that by merely focusing on the relevant authorities (those with a statutory duty to pay regard to the SC Code) the impact of the SC Code itself might be less effective. This is because the SC Code covers standards, audit, good practice, transparency and data protection requirements. It is therefore important to include all key stakeholders in the effort to improve standards across the broad user base.

In February 2016 I presented to the Government my *Review of the Impact and Operation of the Code* (February 2016). This review was a commitment made by Ministers during the consultation phase of the Protection of Freedoms Bill. I upheld that commitment and made the following recommendation (recommendation 7):

> *"The government should consider ways to incentivise such organisations with a significant 'surveillance camera footprint' to voluntarily adopt the Code."*

Despite some commentators observing that the SC Code should have gone much further and included many other organisations (health, education and transport) I felt that this recommendation provided a measured approach to surveillance camera regulation. The SC Code itself states that:

> *"Para 1.2: … as understanding and application of the code increases, the government may consider including other bodies as relevant authorities who will have regard to the code".*

---

[30] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704479/Strategy_plan_6-_voluntary_adopters.pdf

Further, the SC Code goes on to state:

> *"Para 1.8 … informed by advice from the Surveillance Camera Commissioner, the government will keep the code under review and may in due course consider adding others to the list of relevant authorities pursuant to section 33(5)(k) of the 2012 Act (PoFA)."*

Given the introduction of the Data Protection Act 2018 I specifically raised with the Home Office the imperative that the SC Code be reviewed in its entirety. The SC Code incorporates requirements that are intrinsically linked to the Data Protection Act 1998 and needs urgently to be refreshed and brought into line with new and existing developments. Having received assurance from the Home Office that this would be done (officials presented to my Advisory Council outlining their commitment to deliver a review of the SC Code within the reporting year) I subsequently discovered this work had been halted owing to competing pressure (Brexit was advanced by one senior official). The Home Office Biometrics Strategy now commits to conducting this review and I remain hopeful that an anticipated start date of early autumn 2018 will commence the process.

## National Health Service and Other Public Bodies

Within the aforementioned *Review of the Operation and Impact of the Code* (February 2016) I made the following recommendation (6).

> *"The scope of relevant authorities within PoFA is expanded to cover all public bodies in receipt of public monies or publicly funded in any way. The Act should apply to any authority using overt surveillance in public space that has obligations under Human Rights legislation and/or capabilities under Regulation of Investigatory Powers Act 2000 (RIPA)."*

I was told by government ministers in March 2016 that the Information Commissioner had powers to enforce the SC Code.This of course is not the case. The PoFA gives no statutory role to the Information Commissioner in relation to the SC Code. The Information Commissioner does have powers in relation to the Data Protection Act 2018, and elements of that Act are incorporated within the SC Code. For that reason we have drafted a memorandum of understanding that has recently been refreshed.[31]

I have continued to put forward arguments to Government to support the consideration of the National Health Service (NHS) being brought into the auspices of a relevant authority under the PoFA. The arguments for so doing focus upon the introduction of new and advancing technology, the potential vulnerability of patients and families attending NHS premises and the sheer number of people who pass through those premises:

- the total number of attendees at accident and emergency departments was 22.9 million in 2015/2016; and
- there were 15.9 million total hospital admissions in 2014 and 2015.

[31] https://www.gov.uk/government/publications/memorandum-of-understanding-surveillance-camera-commissioner-and-information-commissioner

The argument that is put back to me is that data protection legislation is sufficient to regulate the use of surveillance cameras in the NHS. Rather than support the Home Secretary's SC Code I am told there is no requirement to strengthen the SC Code because the Information Commissioner has the powers to provide that reassurance. I respectfully advise that this is not the case.

I am of the opinion that the Data Protection Act 1998 and the Data Protection Act 2018 partially provide a lawful basis for surveillance. They provide a framework for the management of data once the surveillance has been conducted, and a strengthening of the citizens' rights in relation to those data once they have been acquired.

Hospitals are increasingly using video surveillance systems incorporating drone technology, body worn video cameras and automatic number plate recognition (ANPR) systems. It is reasonably foreseeable that the advent of automatic facial recognition for access control, the protection of vulnerable sites and myriad other issues will ensue.

The rationale behind introducing the SC Code is:

- to reinforce the oversight of public space video surveillance; and
- to provide confidence and reassurance to the public that the relevant authorities were adopting the highest standards.

Indeed, my role was introduced despite the existence of the Data Protection Act 1998 having been in existence for 14 years.

Taking the comments that I have received from Government it certainly creates the perception that the PoFA and the SC Code are not seen as a method to regulate surveillance going forward. This is short-sighted in my view. I am seeing increasing arguments and debate around the legitimacy of surveillance camera systems, particularly given the advent of artificial intelligence and its new and increasing capabilities.

I am sensitive to the argument that the NHS is under operational and financial pressures and that it will not benefit from added regulation. However, I have consistently stated that adopting the SC Code as a relevant authority will not require a surgeon to leave the hospital theatre to attend to the surveillance cameras protecting the sites. Every NHS has a security infrastructure to safeguard its patients, visiting family and friends, buildings, infrastructure, medicines, toxins, radiological substances, and so on. Accordingly, the NHS has the security apparatus to oversee that operation. The leadership and example of Barnsley Hospital NHS Foundation Trust, in being the first NHS Trust to voluntarily adopt and receive my independent third-party certification remains an example to others.[32] I am also delighted to report that, during the year, the Great North Air Ambulance service also received full certification.

## Universities and Education

There are similar arguments to be explored amongst the thousands of educational establishments across England and Wales as to those made in relation to the NHS.

These establishments aim to provide safe spaces for their students. The use of legitimate, well-managed and properly regulated video surveillance systems is a priority if they are to be used at all. I am seeing a growth in the use of surveillance in those establishments

[32] https://www.gov.uk/government/case-studies/barnsley-hospital-nhs-foundation-trust-get-certified

and its use in changing room areas and toilets continues to acquire news column inches. It is also reasonably foreseeable that advancing technology will become increasingly attractive to those establishments. Facial recognition, drone technology and other software additions – some as yet unimagined – are likely to be on the horizon in the not too distant future.

I will continue to call the Government to review the SC Code and include these establishments within the list of relevant authorities that must pay statutory regard to the SC Code. Many universities boast a transient student population that is equivalent to a small town. Is it right, given the inherent vulnerabilities of these students, that there is no enhanced requirement under the SC Code for universities to comply with high standards? Further, it is possible to compare these institutions operating hundreds of cameras in public spaces (utilising advanced technology) with a parish council that might be operating a solitary analogue camera. The parish council operates under the regulatory SC Code; the university does not.

I have enjoyed excellent co-operation from the Association of University Chief Security Officers, having been invited twice to present at their annual national conferences on the matter of surveillance on campus. I have also continued to work with Universities UK, which has provided details of the SC Code to their members.

I am also delighted to highlight that this year Oxford University and the Universities of Worcester and Wolverhampton have successfully achieved third-party certification against the SC Code. It is of note to highlight that a consistent message I receive from all these organisations is 'make it mandatory' and it will be much easier to ensure that compliance is attained and standards are driven up. That is my challenge to persuade the Government as to the merits of the argument.

## Parking Industry

I see this sector as an opportunity to seek to raise standards on behalf of the public and in the public interest. Arguably there is nothing as vexing for a member of the public receiving a parking violation prompted by the use of a video surveillance camera and increasingly by use of ANPR systems. Anything to seek to drive up the standards of its use, deployment and technology would be valuable in enhancing public trust and confidence in its use.

The British Parking Association (BPA) is the largest professional parking association comprising around 700 organisations. Its members comprise technology developers, equipment manufacturers, training providers, and so on. After several months of engagement, discussions and presentations to senior Board members I am delighted to report that earlier this year the BPA launched the requirement to comply with the SC Code within their own Approved Operator Scheme Code of Practice, particularly Clause 21.5:

> *"We have an expectation that when Operators are using cameras to manage parking, they will sign up to the Surveillance Camera Commissioner's Code of Practice and adopt Guiding Principles which are detailed in Appendix F of the Code."*

Indeed I felt this was a significant achievement and on 14 March, 2018 I blogged about it.[33]

---

[33] https://videosurveillance.blog.gov.uk/2018/03/14/positive-progress-with-the-parking-industry/

This constitutes important progress. To acquire data from the Driver and Vehicle Licensing Agency (DVLA), parking companies have to demonstrate that they comply with BPA regulations. The BPA has highlighted that it expects these companies to comply with the 12 Guiding Principles of the SC Code. I intend to use this commitment as a vehicle to support the BPA in holding those operators that do not so comply to account.

Operators should now include processes of annual evaluation and review of systems – the absence of which contributes significantly to poor surveillance practices. It is early days but I will be working with the BPA to monitor this initiative, particularly to see how many of those organisations publish their adoption of the SC Code and acquire certification. The BPA has 37 operators that use ANPR and has contacted them all to encourage sign up to the SC Code. A total of 19 operators have signed up to the guiding principles. Earlier this year Defence Systems Ltd, trading as Park Wark, was audited by the Security Systems and Alarms Inspection Board and achieved a full certificate valid until 27 March 2023.

This is excellent news and follows on from the work of the International Parking Community (IPC), which is the newest accredited trade association in the private parking sector. The IPC incorporated the SC Code into its accredited operator scheme last year and was reported in my 2016/2017 Annual Report.

## Retail

Retail, of course, is a major stakeholder in the usage of video surveillance cameras. The reader will see from the delivery plan[34] that, in terms of voluntary adopters, I have focused specifically on this sector.

The strand lead for the National Surveillance Camera Strategy, Philip Jones, a security manager at Westfield Europe Ltd, has been influential in engaging the broad retail security ecostructure in promoting the SC Code. Early in the reporting year he had secured the commitment of Revo (Security and Shopping Committee), the British Retail Consortium (BRC) and the Association of Town and City Management (ATCM) to raise awareness of the SC Code. I am advised that organisations within these structures are completing the self-assessment tool. However, at this stage, I have no independent and auditable method to evidence that. I shall continue to work with these sectors and look towards defining an empirical method of demonstrating this progress. The importance of this development is increasing, given the emerging use of advanced technology, automatic facial recognition (AFR) and ANPR within this sector.

Given all of the above I remain concerned about the impending use of the equipment. My office has intervened in the proposed use of this type of equipment in a police environment. Following our concerns this pilot was halted until greater assurance could be offered regarding compliance with the SC Code. You will recall that the SC Code provides that the Surveillance Camera Commissioner will be a source of validation for the use of such systems (including AFR). In these circumstances this means complying with the SC Code. I have no doubt that in due course the judicious use of AFR will become a valuable tool in society – but its legitimate use (necessity and proportionality) will act as a magnet for scrutiny and criticism.

---

[34] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704479/Strategy_plan_6-_voluntary_adopters.pdf

# Chapter 7 – National Surveillance Camera Strategy for England and Wales – Installers, Designers and Manufacturers

The video surveillance camera industry comprises a range of organisations of varying complexity. Many such organisations operate globally and from outside the UK. This sector is clearly influential in standards setting when considering the use of video surveillance systems (VSS). Yet, to what standards do they seek to adhere and how are those standards policed?

The answer to that question still remains fairly loose. Of course British, European and International Standards exist for VSS but are too infrequently mandated as being part of an operation requirement for purchasers of such systems. In view of these complex arrangements the National Surveillance Camera Strategy[35] recognised that a key way to influence manufacturers to adhere to recognised and known standards was to produce a 'Buyers' Toolkit' that would seek to influence such adherence. Failure to do so would hit the bottom line of companies seeking to supply the home market.

The British Security Industry Association (BSIA) is leading the project on behalf of the strategy and is due to publish in summer 2018. The Buyers Toolkit will be an easy-to-follow guide for non-expert organisations that:

- are thinking about buying a surveillance camera system; and
- want to ensure that they buy an effective system that does what they want it to do.

The Buyers' Toolkit is aimed at small- and medium-sized enterprises (up to 250 staff) and micro-businesses (up to 9 staff). It will help people to make informed decisions about whether surveillance cameras can be justified as a solution to their problems. If surveillance cameras are necessary, then the toolkit will provide advice and guidance on how people can work with prospective suppliers to ensure that a system is installed that meets their requirements.

I believe that this will be a significant milestone for the strategy and will demonstrate the power and impact of co-ordination across the various stakeholders in driving up standards and retaining public confidence in public space surveillance. To demonstrate that point, this work has leaned heavily on the standards strand of the strategy to ensure that relevant standards are incorporated within the toolkit. Additionally, it is important for the toolkit takes account of cyber related issues via our cyber expert, Mike Gillespie, so that relevant advice can be provided to the purchaser. My thanks to Jacques Lombard (Chair of the BSIA video surveillance section and Managing Director of Syntinex Security Systems) and Alastair Thomas for driving this work forward and harnessing the great experience of a wide range of organisations to deliver this project.

---

[35] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704487/Strategy_plan_8-_installers_designers_and_manufacturers.pdf

# Chapter 8 – National Surveillance Camera Strategy for England and Wales – Training

The relevance of high-quality training to driving up standards is self-evident. I am grateful to Gordon Tyerman for driving this objective on behalf of the National Surveillance Camera Strategy[36]. As training spans a number of the strands of the strategy Gordon has been not only delivering his own strand, but also supporting others.

As we continue to see new legislation, develop new standards and new guidance regarding advancing technology it is important that we harness this sector within the industry. I look forward to reporting next year on some of the developments that follow on from the successful 'gap analysis' that we have conducted across the training sector.

One of the key areas will be to provide access to relevant training courses on my website, which will be achieved in the reporting year.

Currently, the only compulsory training for CCTV operations is for the Security Industry Authority (SIA) licence issued under the Private Security Industry Act 2001 for contracted front-line operators of CCTV surveillance equipment in public spaces. We are working with the SIA on updating this training, which will raise the level of the skillset required.

Across the remaining roles within the surveillance camera industry, there is a desire to raise standards, but the availability and level of training courses is sporadic and there is no requirement for compulsory training. I strongly believe that the designers, installers and managers of CCTV surveillance systems should have access to training that is appropriate and set at the correct level for us to benefit from the immense investment made in CCTV surveillance systems. With the assistance of specialists in the CCTV surveillance industry and awarding bodies, we are making progress in identifying suitable and appropriate training methods.

With the changes in technology and the risks posed by internet access to images, practitioners of CCTV need to be able to appease any fears that the public may have on our use of cameras. Having a robust framework of training in the UK will allow us to achieve standards that will be the envy of the rest of the world.

---

[36] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704512/Strategy_plan_9-_training.pdf

# Chapter 9 – National Surveillance Camera Strategy for England and Wales – Regulation

As the reader might expect surveillance attracts the focus of regulators from a variety of perspectives:

- covert use by state agents attracts the focus of the Investigatory Powers Commissioner;
- use by the police is a legitimate interest of Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services;
- increasingly the Biometrics Commissioner is engaged upon the use of biometric modalities (facial recognition, gait analysis, and so on);
- the Forensic Science Regulator is engaged where appropriate; and
- the Information Commissioner's Office (ICO) is engaged in terms of how the data is processed.

Underpinning all these interests is the Regulators' Code,[37] which sets the public interest as being paramount. Accordingly I have set a specific objective within the National Surveillance Camera Strategy[38] to enable the regulators to co-ordinate with fellow regulators, harness shared thinking and develop an understanding around areas where further consideration needs to apply.

Fellow regulators have agreed our first scheduled meeting in the next reporting year (2018/19) and I look forward to explaining developments in tandem with my colleagues. In advance of that meeting I am pleased to report that, together with the ICO we have refreshed our memorandum of understanding to reflect better the developments of our respective engagement in the field of video surveillance camera systems. I am also pleased to report that, together with the Forensic Science Regulator, we have created a new memorandum of understanding.

As the sophistication of video surveillance technology advances, the interplay between different regulatory approaches is brought into focus. The challenge brought about by the introduction of facial recognition technology is a case in point. I reported in last year's Annual Report that it required a new paradigm of legislation and regulation to manage those challenges.

The increasing power of the commercial sector in utilising surveillance technology, and its complex relationships with law enforcement, underpin those challenges. The ability of overt surveillance operated by private enterprise to cross reference and data mine against a variety of databases presents a challenge to both the Government and society. It is important that the mantra of 'just because you can, doesn't mean you should' needs to be applied. Careful thought around how these challenges are to be managed going forward is required.

---

[37] https://www.gov.uk/government/publications/regulators-code

[38] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/704619/Strategy_plan_10_-_regulation.pdf

I look forward to the review of the Secretary of State's Surveillance Camera (SC) Code of Practice (announced in the Home Office's Biometrics Strategy) and seeking to ensure that those challenges and range of solutions are reflected within the revised SC Code.

Over the course of the year I have strengthened relationships with my fellow regulators both at a strategic and working level. As I set out in the policing chapter of this report – these relationships are extremely important in order to provide a constructive challenge to those wishing to use ever invasive video surveillance systems. The aim is to ensure that citizens are kept safe, but not at the price of their right to privacy.

Much of the work on the regulation strand of the strategy was led by my Head of Policy and Support, David Buxton. I must thank David in this report – the contribution that he has made to this strand and to the strategy in general has been significant and he must take the credit for that. He will have retired by the time this report is published and I wish him all the best in his retirement.

# SURVEILLANCE CAMERA COMMISSIONER

CCS1218140748
978-1-5286-0972-2