SURVEILLANCE CAMERA COMMISSIONER

Annual Report
2018/19

Surveillance Camera Commissioner Annual Report 2018/19

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

June 2020

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: 978-1-5286-1917-2

CCS0420516330 06/20

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 sixth Annual Report covering my regulatory activities from 31 March 2018 up until submitting it to you.

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

- My police survey shows use of integrated and highly sophisticated video surveillance platforms will continue to increase. The public will expect the police to maximise the value of this technology to help protect them and keep them safe. A cornerstone of this debate has been the use of facial recognition technology and the Government's commitment to refresh the Surveillance Camera Code of Practice and governance of biometric technology and surveillance. At the time of writing, this has not yet been published. This must be addressed at the earliest opportunity to increase confidence.

- Last year I reported that the overlap between police use of video surveillance platforms will become more connected to that of private and commercial organisations. The aforementioned survey indicates there is a lack of strategic grip by chief constables on the nature and extent on these partnerships. Reporting of use of biometric technology at Kings Cross, Meadowhall and Trafford Centre shopping centres underscore that issue. As the Government moves towards recalibrating governance of biometric technology, it is – in my view – important that equal focus is placed upon the nature and extent of police surveillance and its broader impact, than simply enabling a much broader use of such technologies amongst both public and private sectors. Their requirements are not necessarily mutually supportive.

- The pro bono work and effort of leaders across the video surveillance industry to support the National Surveillance Camera Strategy for England and Wales continues to deliver quite remarkable support and has delivered key successes highlighted within this report. This report will again demonstrate the breadth and depth of that work. This report highlights the inadequate support and investment the Government has contributed to this work. The Strategy delivers a full and comprehensive approach to the issue of public space surveillance cameras and has secured the support of ten industry experts, all providing their expertise free of charge, to develop strategies, policies and best practice. Last year I challenged the Government to recognise this support and provide real and meaningful resource to help enable its delivery. This has not yet been forthcoming; in fact, the size of my support team has

shrunk. This report provides a more comprehensive schedule of the resource provided and provides a strong assessment of what is required.

- I must reiterate the calls I made in my previous reports for an extension to that Code. 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 Code in achieving its purpose of driving up standards in what is increasingly an agenda that attracts significant public attention and debate.

- I was grateful for the High Court granting permission for my 'intervention' in the recent court case (Bridges v South Wales Police) concerning live facial recognition technology. The judgment, now subject to appeal, highlights an argument that I have been presenting to the Government for several years. Its use concerns much more than privacy and data. Its use extends far beyond the remit of the new Data Protection Act 2018 and concerns the appropriate use of relying on common law and a complex web of laws and precedents. I still believe that the answer relies upon the Government developing a more robust Surveillance Camera Code of Practice. That Code should incorporate stronger guidance as to the authorisation and use of such technology. It should remain principle-based and, unlike views expressed by other commentators, I do not believe we need a code for every biometric or surveillance modality. We do need a strong principle-driven approach that enables relevant authorities to ensure the use of such technology is lawful.

It has been another successful and extremely busy period for my office. I am indebted for the continuous support they have provided and look forward to supporting the Government in determining how these very important agendas will be managed going forward.

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 2018 to 31 March 2019. In addition, it also covers any key issues that have come to the fore from 31 March 2019 until the date of publication.

I provided my first report last year on the National Surveillance Camera Strategy (NSCS) England and Wales, which I launched 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.[2] 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. It now comprises 11 works strands, each being led by an industry expert, and a comprehensive delivery plan reflects the ambition and timescales for delivery.

To ensure efficient and effective management of the burgeoning business areas crossing my desk, I have merged the Advisory Council with the management group which develops the NSCS. This prevents duplication of work, but I have ensured that all previous equities are represented within the amalgamated group.

This report continues to reflect the ambitions and outputs of that Strategy. The NSCS has recently (March 2019) had its second annual review and is a prevailing theme throughout this report. The Strategy provides a vehicle to improve standards, which was one of the key aims of the legislation (PoFA) that introduced the role of the Surveillance Camera Commissioner.

A consistent refrain I recite at the many conference speeches, media interviews and workshops I attend is the importance of transparency and openness in the use of public space surveillance. To that end I continue to believe that Parliament must have visibility on the outcomes and outputs of this work. A detailed résumé of our efforts within the NSCS are documented herein. 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 video surveillance technology is delivering value for money and the NSCS seeks to evidence that assertion; 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) who must pay due regard to the Surveillance Camera Code of Practice (SC Code) are complying with the requirements of PoFA.

[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

Surveillance, never far from the public eye, has been catapulted to the top of the agenda with the court case between Bridges (Liberty) v South Wales Police over the police use of live automatic facial recognition (AFR) linked to video surveillance systems. I 'intervened' in this case and highlighted to the Court that my role, and the SC Code I oversee, represents a key foundation of the law that enables the use of such technology.

The verdict in the case was released in September 2019. In essence, it confirmed its view that, in certain specific circumstances, the use of this technology is lawful. As I write, this verdict is being appealed and will be heard at the Court of Appeal in 2020. I intend to 'intervene' again. The consequences of this case cannot be overstated. It speaks to the type of society we wish to live in, the level of intrusion that is permissible, and the balance between security and privacy. It is right that the matters inherent are scrutinised by the Court in public.

Readers of my previous annual reports will recognise that I have been calling upon the Government to recognise these shifts in usage and develop a new paradigm for the management of technology-driven surveillance systems that have the capability and capacity to infringe on civil rights. Yet, at the same time, can provide significant benefits to society if used proportionately. In speeches and blogs I have alluded to the very firm foundation that covert surveillance enjoys under legislation such as Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016. As overt surveillance becomes capable of increasing intrusion, it is important that this lacuna is addressed if public confidence is to be maintained.

In my 2017/2018 Annual Report, I reported as follows:

> "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, PoFA and the Regulation of Investigatory Powers Act 2000."

I have been consistent in my assertion that Government must address this issue and provide greater reassurance to the public that surveillance in the public space is effectively regulated. The outcome of the aforementioned court case will, I assume, provide that certainty. In the meantime I would urge the Government to deliver upon its commitment in the Home Office Biometric Strategy where, as a key deliverable, it committed to refresh the SC Code. Progress against this objective is glacial and worryingly suggests a lack of commitment in this area. 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 which sets out the arguments and challenges to the use of this equipment. The Home Office Biometric Strategy does represent recognition by the Government that the rapid march of such advancing technologies requires a degree of harnessing across policy and

lawmakers. Indeed, the Court in Bridges took cognisance of the Government's intention within this Strategy to review the SC Code.

It is interesting to read back through my previous reports to Parliament. In my 2017/2018 Annual Report I commented as follows:

> "New technology challenges the legal basis or legal justification of this technology. Automatic number plate recognition systems (ANPR), AFR 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 legal 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 linked systems to sensor and video surveillance technologies with complex reference databases. The capability and capacity of this technology creates new challenges. When combined and integrated, they are potentially 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 also refer to the expansion of relevant authorities (recommended in the 2016 review to ministers);[3] there is a clear argument for all public sector organisations to become relevant authorities within PoFA. For example, hospitals will typically be operating hundreds of surveillance cameras on their premises – CCTV in their buildings, body-worn video on security staff, ANPR in their car parks, and I have even heard of some hospitals looking into AFR. The NHS treats millions of patients, arguably at their most vulnerable, who are exposed to ever-increasing surveillance technology. I have been told by the Government that the new Data Protection Act 2018 (DPA) provides the relevant reassurance that these cameras are justified and being operated effectively and proportionately. In my view, this is not persuasive. I reiterate that statement and draw the distinction between the conduct of surveillance and the processing of data as a result of that surveillance.

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? I continue to argue that organisations such as Transport for London, the Highways Agency, education establishments, rail franchises, government departments and the critical national infrastructure should, as an absolute minimum, be included as relevant authorities within the PoFA. I

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

reiterate that it is 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.

An exciting development this year has been the introduction of a new work strand within the Strategy. I am delighted to welcome Professor Pete Fussey (Director at the Centre for Research into Information, Surveillance and Privacy (CRISP) and Professor in Criminology at the University of Essex) to the team and the Advisory Council. Pete is developing the strand under the banner 'Human Rights, Data and Technology'. Fresh potential exists to mine information on citizens living in an increasingly data-rich society. Whilst such advancements have undoubted advantages for pursuing public safety, it is important their use remains proportionate, fair and accountable to the rule of law.

Within this space it possible to see a critical tension at play. Developments in surveillance equipment make effective regulation more important than ever before. Yet the complexity of this technology makes these forms of oversight increasingly challenging. At the same time, many existing legal, regulatory and oversight mechanisms are in a state of flux. On one hand, many forms of regulation were written long before some current forms of video surveillance were imagined. An absence of case law concerning many recent forms of surveillance adds further uncertainty. On the other hand, attempts to place advanced forms of surveillance on a legal footing, such as the Investigatory Powers Act 2016, have generated significant debate and seen their foundational ideas challenged in recent rulings of the Court of Justice of the European Union and European Court of Human Rights.

The task for regulators to ensure responsible and fair uses of surveillance commensurate with the principles of democratic society, then, is a necessary yet difficult one. Pete will engage in constructive dialogue with a range of important stakeholders including other regulators, civil society groups, legal experts and, crucially, those who use surveillance cameras to promote public safety.

The new reporting year presages the increasing impetus I am placing around citizen engagement. I am privileged to have Professor William Webster developing this strand of the Strategy. Last year we held the first Question Time styled event 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. I will look to hold a similar event in 2020.

A National Surveillance Camera Day took place on 20 June 2019. The aim of the day was to encourage a conversation about the use of surveillance cameras in modern society. Love or hate such surveillance, it is right the people have an

opportunity to see it, discuss it and assess for themselves how technology is driving its use forward.

The event itself was a major success. Combining this day with the launch at IFSEC (the leading integrated security event in UK and Europe) of the new Secure by Default certification process gave the event the platform it deserved. National media engaged and a variety of events took place across the country.

The delivery of the 'Secure by Default' self-certification for manufacturers,[4] which was launched at IFSEC 2019 (a major work piece throughout the reporting year), is aimed at enabling manufacturers to state they meet minimum cyber security requirements at the point of manufacture of video surveillance systems (VSS), or manufacturing or assembling components intended to be utilised as part of a VSS. This scheme is, I believe, the first scheme globally to take this approach and will help ensure cyber security integrity of VSSs. I have set clear pathways for driving up standards within the video surveillance industry. This approach is inexorably linked to the publication of our Buyers' Toolkit last year which continues to receive positive support across the sector.

I am delighted to present this report which truly reflects the hard work and commitment of so many professionals, security experts, civil rights groups and, particularly, the senior leaders who comprise the strand leads on the National Strategy. Those strand leads provide their energy and commitment free of charge and have, in the preceding two years, helped to raise standards of public space surveillance enormously. I am of course also extremely grateful to my small team (Mick Kelly, Katie Scotton and Ola Akande) for their support and challenge. I will endeavour to capture that immense effort throughout this report.

Resources

For the reporting year, my resource allocation comprises an annual budget of £300,000.

It is appropriate to consider the issue of resources that support my role. At times in the reporting year, I have operated at a 25% to 50% reduction in staffing due to people moving in to other roles and going on maternity leave without being able to backfill vacancies. Elsewhere, my team and I have had to go through laborious and bureaucratic processes to bring on board agency staff and an expert consultant to ensure that we are not subsumed by our ever-increasing workload – this alongside the recruitment campaigns we are running to fully staff the office.

Whilst the Home Office and the Government support the Strategy, and given that its very objective supports the Home Office single departmental plan – 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

[4] https://www.gov.uk/government/publications/secure-by-default-self-certification-of-video-surveillance-systems

the limited resources, the failure to ensure backfilling of staff has placed a tremendous strain on the remaining personnel.

In the 7 years since PoFA was enacted, there has been a surge in the use of surveillance platforms being used by relevant authorities and the private sector, yet my resources have stayed static. At Annex A is an outline of what resources I believe are required for this role to be fully supported.

Chapter 1 – NSCS for England and Wales – standards

This strand of the NSCS is led by Alex Carmichael, Chief Executive of the Security Systems and Alarms Inspection Board (SSAIB). Alex is supported by a strategic group whose representatives span the whole spectrum of the industry. The focus of PoFA is to ensure that public support and confidence in public space VSS is maintained and enhanced.

Principle 8 of the SC Code 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."

Certification schemes

In previous years I have focused on the success of the introduction of third‑party certification for operators of video surveillance camera systems. For transparency I now publicise on my website those organisations who are achieving this certification.[5]

Future developments are now focusing on the complex supply chain to develop linkages between the operator and the rest of the process. For service providers (installer, integrators and consultants), we are putting together requirements based on current good practice, using the applicable standards stated on my website.[6] 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. The standards strand is using the NPCC policy for the draft service requirements, as many video surveillance service providers are currently certificated to these. The strand has produced draft requirements for a service provider and formed a stakeholder group made up of the relevant industry trade associations, inspectorates and expert members. This project is ongoing and the aim is to have a certification scheme ready towards the middle of 2020.

The strand is also developing a certification scheme for surveillance camera monitoring centres. Again, this is to support principle 8 of the SC Code and to ensure that monitored VSS are operating to relevant standards. The scheme will cover the

[5] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme/list-of-organisations-who-have-received-the-surveillance-camera-commissioners-third-party-certification-mark

[6] https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry#guidance-for-in-house-monitoring-centres

two types of monitoring centre (there is also a Contract Monitoring Service which may provide personnel to the two types of monitoring centres):

- Contracted monitoring centre – this is where a surveillance camera system owner contracts out the monitoring of their surveillance camera system.
- In-house monitoring centre – This is where a surveillance camera system owner monitors their own surveillance camera system.

The scheme should be launched close to the launch of the service provider certification scheme in 2020. A third scheme for consultants is also in development but working to a slower timeframe and should be launched in 2021.

Secure by Default – self-certification

I am delighted to report that at IFSEC 2019 I was able to launch Secure by Default, minimum requirements for manufacturers of surveillance camera systems and components.

Driven by the need to ensure the UK's resilience against forms of cyber security vulnerability, as well as to provide the best possible assurance to stakeholders, the new minimum requirements are an important step forward for manufacturers, installers and users alike.

The work has been led by Mike Gillespie (Advent IM) and Buzz Coates (Norbain) and developed in consultation with manufacturers (Axis, Bosch, Hanwha, Hikvision and Milestone Systems). It has been designed by manufacturers for manufacturers.

If a device comes out of the box in a secure configuration then there is a good chance it will be installed in a secure configuration. Encouraging manufacturers to ensure they ship their devices in this secure state is the key objective of these minimum requirements for manufacturers. Manufacturers benefit by being able to demonstrate they take cyber security seriously and their equipment is designed and built to be resilient. Installers and integrators benefit from the introduction of the requirements by not having to know how to turn dangerous ports or protocols off during the installation. End users benefit because they know they are buying equipment that has demonstrated it has been designed to be resilient to cyber attack and data theft.

Manufacturers can demonstrate they meet the minimum requirements by completing a self-certification form and submitting it to my office for validation. If successful they will be able to list the component or system as certified by me and will be able to display my certification mark.[7]

[7] https://www.gov.uk/government/publications/secure-by-default-self-certification-of-video-surveillance-systems/organisations-who-have-been-given-our-secure-by-default-self-certification-mark

It has been an enlightening and positive experience working with manufacturers toward a common goal and it is a genuine world first and further Secure by Default for manufacturers will follow over the next couple of years. There is also a Secure by Default for VSS installations in development.

Running through this certification 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 my logo, which is already nationally recognised.

Guidance for in-house monitoring centres

Last year I reported on the significant progress made by this strand including the planned introduction of best practice guidance for in-house monitoring centres to demonstrate how they should secure, manage and operate such a centre and thereby meet the principles in the SC Code. I am delighted to report that this was published on my website in October 2018.[8] It was designed in conjunction with the National Association of Surveillance Camera Managers (NASCAM) and is a significant step to drive up standards across the surveillance camera industry. This enables in-house monitoring centres to understand and execute best practice in respect of their surveillance camera systems and adhere to legal requirements. I am extremely grateful to Ilker Dervish (NASCAM) for leading this work.

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747707/4851_HO_Surveillance_Camera_Commissioner_-_Inhouse_monitoring_centres_180918_V3.pdf

Chapter 2 – NSCS for England and Wales – civil engagement

In developing the NSCS I was determined to deliver upon the governments promise 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."[9]

At a time where new technologies are increasing exponentially, their capabilities are arguably 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 use is paramount.

Professor William Webster (Director of CRISP and Professor of Public Policy and Management at the University of Stirling) leads the civil engagement strand of the Strategy. Professor Webster is a leading academic in the field of surveillance and privacy. In devising the objectives for the delivery plan he has set deliberately challenging goals. His view is that if the Strategy is to have credibility it must be seen to embrace the negative comments about the use of surveillance cameras as well as the positive to enable a true debate to develop.

The key achievement of the year was undoubtedly the world's first Surveillance Camera Day on 20 June 2019. The aim of the day was to encourage a conversation about the use of surveillance cameras in modern society. It was organised by Professor Webster with support from my office. We were not promoting any one message or position on the day. What was most important was to encourage debate about surveillance cameras from anyone who had an interest. We did this by:

- encouraging surveillance camera control centres to throw their 'doors open' so that the public could see, first hand, how they operate;
- asking control centres to publish information about how and why they use surveillance cameras – and to publish the basic facts about their systems on a template we had designed;
- encouraging organisations to publish information about surveillance cameras on social media – we issued a media pack, including logos and imagery, to assist with this;
- issuing press releases and working with media outlets to publicise the day;

[9] Paragraph 1.5, Secretary of State's SC Code.

- blogging and drafting articles in relation to the day;
- launching 'Secure by Default' minimum requirements for manufacturers at the IFSEC International Conference in London.

A media pack was developed to assist organisations in promoting messages regarding surveillance cameras and their use. It included information about the day and what initiatives were taking place, key messages, branding and quotes for press releases. Feedback from stakeholders was that the pack was useful. We also made information available for use on the day on my website.[10]

In the lead up to and on the day there was significant press activity, much of which was a result of the press releases that were issued – this included articles in mainstream broad sheets such as *The Times* and *The Telegraph* as well as trade press and more niche publications such as Computer Weekly – in total there were 23 articles that referenced the day. Prof William Webster's piece for *The Conversation*[11] was read over 75,000 times.

I also appeared on Radio 5's Live breakfast show which devoted the morning to Surveillance Camera Day and included issues ranging from domestic CCTV, live facial recognition and police use of surveillance cameras. Radio 5 Live has over 5 million weekly listeners. The Day was also covered on BBC2's *The Politics Show* as part of a broader programme about the police use of facial recognition.

Surveillance Camera Day caused significant debate about surveillance cameras on Twitter. The hashtag #cameraday2019 was used in almost 1,500 tweets. Tweets from the Surveillance Camera Commissioner (SCC) about the day had over 95,000 'impressions'. More than half of all police forces put out content via their social media channels and the people and organisations who joined the conversation varied greatly e.g. parliamentarians, civil liberty groups, video surveillance camera manufacturers, installers and the general public. In addition to Twitter, some organisations made videos regarding how they use surveillance cameras and posted them on YouTube, receiving 620 views.

We encouraged control rooms to members of the public via our 'doors open' initiative. We know of 12 organisations that took part with around 250 visitors. Those that participated included local authorities, police forces, universities and hospitals. Feedback was that it was a valuable experience for people who attended and the organisations learned from it too. We were not prescriptive about how these events were organised. Some chose to open up to any member of the public and others opened to specific groups such as schools. Also, some organisations thought that they could not take part as they were concerned they would be opening up control

[10] https://www.gov.uk/government/publications/surveillance-camera-day-20-june-2019
[11] https://theconversation.com/surveillance-cameras-will-soon-be-unrecognisable-time-for-an-urgent-public-conversation-118931

rooms to people they did not want in them (e.g. criminals). Some went so far to say we should not be promoting the initiative and that it was a security risk.

We developed a factsheet template which was available for organisations to download from the SCC website, complete it with details of the surveillance camera systems they own and publish it on their website. The factsheet has been downloaded from the SCC site 379 times since it was published, although we have no feedback on whether organisations used it.

As I mentioned in Chapter 1 on standards, we launched the Secure by Default minimum requirements for manufacturers of surveillance cameras at IFSEC on Surveillance Camera Day 2019. This was successful as we could tap into the IFSEC communications team to promote the day.

An immense amount of work took place to deliver this objective. We work with a range of organisations to promote and get involved with the day – police forces, local authorities, manufacturers, civil liberty groups, the Information Commissioner's Office (ICO), and a vast of array of public and private surveillance users, operators and industry specialists.

There remains significant support for technology that can keep us safe. Police use of ANPR and local authority cameras were profiled throughout the day by both organisations. There is increasing transparency around its use reflecting the impact of the SC Code and willingness of police chiefs and local authority chief executives to increase visibility of its use.

Surveillance Camera Day 2019 can be considered a great success and we are planning to repeat the day in 2020. A national conversation was realised through the activities delivered. This has contributed positively to further debates about surveillance cameras, in particular in relation to AFR systems and the regulation of contemporary systems. Whilst most elements of the day worked well there are a number of lessons learned that can inform delivery in 2020:

- The media pack and graphics were well received and used, and are designed for re-use in future years.
- Announce the date of the day earlier than we did in 2019, which was roughly three months before. We had feedback from some organisations that they need longer lead-in time to plan communications and activities. Our suggestion would be six months in advance.
- Develop a more robust planning process. Whilst our planning was effective, using a plan that has more milestones may result in better outcomes as there are lots of elements to the day that need to be managed. For example, the factsheet was only made available two weeks before the day.

- Align the day with IFSEC. This worked very well as we worked with IFSEC to put out messages about the day and meant we could tap into the installer/manufacturer community.

- It was hugely beneficial that third-party organisations like ICO and IFSEC used their communications teams to promote the day. This allowed us to reach a bigger audience and should be repeated in future years.

- As noted above there was some criticism about 'doors open' from some quarters, primarily because there was a feeling that opening control centres to the public was a security risk – given the point of Surveillance Camera Day was about transparency this was surprising. We should develop some case studies from those who took part this year to illustrate how it can be done in a managed way, e.g. by inviting in specific groups such as schools.

- Feedback from police forces is that we may get better engagement if a letter is sent from the NPCC leads and Commissioner to Chief Constables (rather than senior responsible officers for PoFA).

- Much of the work in 2019 was carried out by two people. Consideration should be given to setting up a small working group to deliver the day – possibly made up of: Civil Engagement strand lead, SCC Office, police representative, local authority representative and voluntary adopters representative.

- In 2019 we tried to organise lectures in schools by academic experts. As the date of the day fell in the English school exam period this was not possible. The feasibility of this should be reflected upon for 2020.

Professor Webster is also planning another Question Time event in 2020 which will be similar to that held in 2018 and which I reported on in my last Annual Report. He is also hoping to hold an event in Parliament to raise the profile of the issues with regard to surveillance cameras and their use.

Chapter 3 – NSCS for England and Wales – policing

It is Chief Officers of Police and Police and Crime Commissioners who generate most public sensitivities in respect of overt surveillance camera systems they operate since it is the police who are charged with the responsibility of keeping communities safe from ever evolving threats. The public expect the police to explore emerging 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. The balance between public security and public privacy underpins this debate. Police use must steer clear from disproportionate and illegitimate State intrusion and the public must have confidence that those technologies are being used with integrity. It is for these reasons that the police should be a key strand of work within the framework of the NSCS. Furthermore, Chief Officers of the Police and Police and Crime Commissioners are relevant authorities under PoFA and must pay due regard to the SC Code.

In his 2016 Annual Report, *The State of Policing*, 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."

Indeed, in Sir Winsor's *The State of Policing* he again referred to the police requirement to invest in technology and innovation to make policing more efficient. It is here where the police cut across legislation, regulation and public opinion. Viewing this issue through my regulatory prism the myriad of difficulties faced by the police are apparent. The issues faced within the reporting year concerning Bridges v South Wales Police (use of AFR) effectively highlight the issues.

Automatic facial recognition

This issue has not been out of the media or spotlight throughout the year. The judgment at the High Court was handed down in September 2019.[12] The Court recognised that this case was brought during its trial phase by South Wales Police

[12] https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

and determined that, on the specific occasions in question, its use was "in accordance with the law".

The Court relied upon the current legal framework to explain this judgment; that being the far-reaching scope under common law, DPA, PoFA via the SC Code, and the guidance I issued to police forces in October 2018 (published on my website in March 2019)[13] provided the necessary and adequate legal framework. This judgment is now subject to appeal and we must await determination by the Court of Appeal in this matter. This appeal will be held in June 2020.

Much energy and effort was applied by my office to support these proceedings. In April 2019 I successfully applied to 'intervene' and was grateful for the consent of the Court in so doing. My skeleton argument focused on the element of the legal framework that supported its lawful use. PoFA itself and accompanying SC Code are key elements in ensuring any deployment is 'in accordance with the law'. Additionally, the Court recognised that, together with the SC Code, the guidance I issued is also relevant. I was pleased that the Court accepted, in their judgment, my lead regulatory voice in relation to video surveillance camera systems as follows:

> "The Surveillance Camera Commissioner is the statutory regulator of surveillance cameras".

And:

> "The Surveillance Camera Commissioner's overall submission on the Code was that it provided a "…full system approach to the regulation of surveillance camera systems as it provides the legal and good practice standard which the Government expects, as well as highlighting the broader spectrum of legislative requirements which apply. We agree with that submission."

I agree with this, and this philosophy underpins the working of the NSCS.

The use of AFR will continue to dominate the public attention and focus. The ever-increasing use of AFR in the private sector will continue to be a concern. The increasing use between the private sector and the State is also of concern. In line with my guidance to police forces, I will continue to argue as follows:

- Consult your solicitor before proceeding.
- Consult your authorising officer under RIPA to ensure that legislation does not apply.
- Justify and risk assess your intended use of the technology.
- Engage your community and be transparent in its operation.

[13] https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems

- Keep an exhaustive audit trail of your policies and documents.
- Consult my office to ensure compliance with PoFA.
- Consult your Data Protection Officer to ensure compliance with DPA and refer to ICO if necessary.

One thing is certain, existing surveillance laws will continue to be challenged as technical capabilities grow and State compulsion to use them grows. However, it remains incumbent upon the State 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 SC Code, RIPA and DPA.

Legal obligations

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 have endured for six years. I have consistently called upon the Government to streamline regulatory advice to police (and other relevant authorities) where surveillance platforms are concerned. Since 2000 the 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*.[14] 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 DPA. I understand ICO intend to publish new guidance in 2020 that will reflect the position of data protection post-introduction of DPA and replace *In the Picture*.

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 PoFA 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."

Of course, this overlap existed prior to the introduction of PoFA and it was Parliament's intent to provide for greater scrutiny of relevant authorities in their use of overt surveillance technology. In my report to Home Office Ministers in February 2016,[15] I urged Government to address this and other issues. One can clearly see

[14] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
[15] https://www.gov.uk/government/publications/review-of-the-surveillance-camera-code-of-practice

how complex it is for police to comply with regulation when the complexities themselves are presented within legislative reviews and no action is forthcoming.

I would urge government officials to reflect upon the comments made by Lord David Anderson in his seminal report *A Question of Trust* published in 2015.[16] At paragraph 13.44 he states:

> "My fifth principle therefore, that there should be a single body of law, and a single system of oversight, for equivalent investigatory activities conducted by different public authorities."

It is inescapable that, with overt surveillance using progressively more intrusive capabilities, this aspect of surveillance should be brigaded as marshalled under one oversight body. The increasing overlap between overt and covert surveillance, what it means and how it is conducted, lends further credence to this argument. Indeed, within this reporting year I have submitted evidence to the Investigative Powers Tribunal concerning the capability of overt body-worn cameras to be used covertly by police (AB v Hampshire Constabulary).[17]

Assessment of police compliance with PoFA

Last year I reported upon an assessment of police compliance with section 33(1) PoFA and the SC Code. 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.

I was delighted to note that all 45 Chief Officers responded so fully to the demands I made of them. As a regulator I have no powers of sanction or of enforcement, nor do I seek any. To that end, the police response was remarkable and demonstrates a commitment to operate such technology lawfully and transparently. I made two recommendations that were specific to Chief Officers 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

[16] https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review
[17] https://ipt-uk.com/judgments.asp?id=50

there should be processes in place that enable the police to discharge their responsibilities effectively under the PoFA in respect of those systems."

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

> "It is recommended that the NPCC representative for CCTV considers the workstream being conducted under the umbrella of the NSCS 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."

All relevant police forces now have an SRO appointed and clearly identifiable within each force. The SRO has 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.

This year my office has undertaken another comprehensive review of policing and assessment of compliance with section 33(1) PoFA. I have included a summary of that review at Annex B.

Police engagement in National Surveillance Camera Strategy

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.

Last year I lamented that much of the effort engaging with the police and delivering on objectives within the NSCS had been led by my office and that I looked forward to greater engagement from the police in the coming year. I am delighted to say that that support has been forthcoming. The appointment of Assistant Chief Constable (ACC) Jenny Gilmer from South Wales Police as NPCC lead for CCTV with designated managerial support (Sharon Colley – National Capabilities Manager for CCTV) has started to make a significant impact in delivering the objectives within the Strategy.

As surveillance camera technologies continue to evolve 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 and ACC Gilmer in particular.

The threats to our society are evolving in terms of complexity, technological capability and volume. In the modern age it is likely that the total of those threats will not be countered by personnel increase alone. The police must rely on new technologies including surveillance. The public will expect the police to exploit

technologies to keep us safe, technologies that are in everyday use elsewhere for our convenience. Whilst the challenge of maintaining the balance between public safety and privacy is a perennial issue, I all too often hear the clarion call that the use of technology by the State is 'chilling' or erodes our freedom. Responsibility to engage in reasoned and mature debate has never been so important. This complex issue underlines much of the work we are doing within our citizen engagement strand.

The SC Code clearly defines the route the police must take in this regard 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. I believe the law and regulation is falling behind what is required. The Government's *Biometric Strategy 2018*[18] referred to the refresh of the SC Code. Progress on this is glacial and the Bridges v South Wales Police high court case (use of AFR) provides compelling arguments for Government to advance this work in the public interest as soon as is practically possible.

A key component to the Strategy is the harmonising of function between stakeholders. Since the introduction of CCTV in the 1990s, we have seen local authorities receiving the funding and police being the beneficiary of the product of those cameras.

ACC Gilmer has focused the work on four areas:

- Service level agreements (SLA)
- Ways of working
- Training
- Cloud and artificial intelligence

Service level agreements

A standard set of templates will be devised to provide working principles for forces to use to establish fit-for-purpose agreements with other partners to support all round beneficial working practices, including the creation of appropriate management information to support benefit realisation.

The establishment of national agreements with major CCTV operators will be built to improve effectiveness and efficiencies in process.

An SLA framework will be created to support collaborative and improved working relations between police and local authorities, which will then expand into other appropriate partners.

[18] https://www.gov.uk/government/publications/home-office-biometrics-strategy

I am delighted that under the banner of the NSCS and the leadership of ACC Gilmer and Tony Gleason (Public CCTV Managers' Association), both organisations are on the cusp of agreeing an SLA framework document. This is essential for the effective and efficient operations of publicly-operated video surveillance cameras. Currently there is a minimal feedback loop between organisations, disparate use of performance measures, and varying practices that do not lend themselves to harmonious function. I am convinced this will help drive up standards in accordance with the objectives of PoFA and it is more fully explained in Chapter 4, Local authorities.

Ways of working

A landscape review will be conducted to understand how forces and law enforcement partners process CCTV footage, and to provide a standard set of working principles that will be developed for each service involved with the processing of CCTV. These standards will be validated by the National CCTV working group members and published to provide transparency. The key objective here will be to ensure there is transparency of process and auditability at all stages of the CCTV lifecycle.

Training

A training capability assessment will be carried out and an agreed updated training package will be devised, reviewing current training practices that are in place across forces and partner agencies, and identifying best practice.

A tiered training programme will be devised to include identified best practice and a continuous competency evaluation framework to support all levels of CCTV involvement. These training materials will extend beyond policing into local authorities, the Crown Prosecution Service, and HM Courts and Tribunal Service, and cover all aspects of the end-to-end lifecycle of CCTV processing.

This work is being coordinated with the training strand of the National Strategy led by Gordon Tyerman.

Cloud and artificial intelligence

Here, there is development of a ground-truthed test data set that can be used for multiple policing purposes and develop learning principles for multiple policing areas, and that can be used by suppliers to test and develop their products to make them fit for purpose for policing.

A technical landscape review will be conducted to scope viability of cloud and artificial intelligence-based solutions, and recommendations for change will be identified, along with the establishment of working relationships with CCTV suppliers and developers to ensure future development is fit for purpose.

The strand is also scoping and documenting CCTV user requirements, including file formats, for a cloud-based solution. Identifying needs at each stage of the CCTV process from capture and acquisition, analysis and exploitation, presentation and sharing and storing and access. This will identify best practice guidance to support police forces in direct uploading initiatives, ensuring these are validated and approved by central government agencies.

Automatic number plate recognition

ANPR continues to occupy a good deal of my time. 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 nearly 20 billion read records is formidable.

At the time of writing, the police are introducing the new National ANPR Service (NAS) which harnesses all the locally-run police systems into one, capable of being operated and administered centrally. As this system continues to merge, it is anticipated that the streamlining of systems and data capture will enhance the capture of vehicle numbers to approximately 50 million per day and nearly 20 billion per year. This system has been described as the largest non-military database in the UK. It has been subject to much media scrutiny and significant commentary from civil liberty groups.

I am delighted to have been asked to continue to chair the NPCC Independent Advisory Group (IAG) by NPCC lead for ANPR, Chief Constable Charlie Hall. This group comprises a variety of interests from civil liberties, motoring industry, regulators, Home Office, lawyers and academics. Minutes and reports from those meetings can be found on my website.[19] This group provides critical oversight to the police and challenges openly and transparently on areas of concern for the IAG. Again, I must offer my thanks to the extremely talented members of the group.

This group enjoys significant access to police and Home Office policy experts. They receive input and briefings on new and proposed changes. Some key headlines throughout the reporting year include:

- **The development of the ANPR Value Model.** This is designed to allow operators of this equipment to understand the economic value provided by ANPR. The work is under development but initial findings look encouraging. The police are responding to criticism regarding the lack of transparency concerning the use of ANPR and the value it provides. The model identifies key ‘delivery areas’ such as arrests, curtailed prosecutions and efficiency savings, and seeks an empirical base to justify its use. Apart from being good governance and supporting community engagement, it is essential in my view to enable the police to demonstrate the ‘necessity and proportionality’ of its

[19] https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about/our-governance

use. This approach will be scrutinised by the IAG and I will report upon the observations made.

- **The National ANPR Camera Strategy.** The police are undergoing a national assessment of the ANPR camera disposition. The aim is to identify areas of duplication or unnecessary siting of this technology. Given that systems, and indeed forces, have merged through regional and strategic partnerships, it is a necessary and detailed piece of work. The aim is to remove any cameras that are not strictly necessary. This approach will further provide reassurance to the public that they are legitimate and necessary. The IAG will scrutinise the proposals and I anticipate much discussion and debate.

- **The establishment of a working group to look at the impact of cloned and defective plates.** It has representatives of the NPCC, the Association of Police and Crime Commissioners (APCC), the SCC Office, Home Office and number plate manufacturers. It is gathering evidence and will present back options to consider what improvement could be made to the life cycle of the number plates and controls around manufacture and sale. The group would be looking at design, enforcement, and impact of cloned and damaged plates.

- **The discussion of initiatives such as green number plates and clean air zones.** The enforcement regimes that sit alongside such developments will use ANPR via local authorities. Will the introduction of these new enforcements lead to individuals attempting to beat them by misrepresenting their plates on their vehicles, e.g. cloned plates, and therefore also impact the police National ANPR system?

There remains much to do. ANPR currently operates under a complex framework of legislation of general application (common law, DPA, the Human Rights Act 1998, PoFA) and policy documentation, but without a single statutory provision. In addition, the police and the Home Office have published the *National ANPR Standards for Policing and Law Enforcement (NASPLE)*[20] as well as audit standards which are thorough and comprehensive.

The use of ANPR 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, monitoring clean air zones and possible enforcement for green number plate initiatives. These fall outside of the scope of police/law enforcement use of ANPR and so are not subject to the rigorous standards that have been developed, so the NAS does not support these uses of ANPR.

There remains limited democratic oversight for such a powerful tool in the policing armoury. Equally, as incentives are rolled out for vehicles which do not pollute our towns and cities and they are policed via ANPR, will it create an environment where

[20] https://www.gov.uk/government/publications/national-anpr-standards

drivers may seek to clone plates or even share plates, which could pose a significant challenge to law enforcement capability? Will they do this if it means not being charged to enter certain zones? As the use of enforcement using ANPR expands, there may need to be tighter controls around who can manufacture plates and when they can be obtained. Such controls exist in many other countries.

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. 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.

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. I do think that the regulators can work closer together on these matters to bring the debate to deliver tangible outcomes to benefit the public interest. Threats to society and to civil liberties are of equal magnitude and are becoming increasingly complex.

My regulatory role oversees public space surveillance. It overlaps with that of Investigatory Powers Commissioner, Information Commissioner, Biometric Commissioner and Forensic Science Regulator.

I recall the observations of Lord Anderson (above) in *A Question of Trust* where he called for all State surveillance to be brought within one umbrella to provide clear and concise governance. I will not state that he specifically had in mind the emerging technological advances but, as they do advance, the argument seems pretty clear. We already have an impressive privacy regulator that oversees covert surveillance in the Investigatory Powers Commissioner's Office (IPCO). There is a persuasive argument to look towards IPCO to provide consistency, reassurance to the public and effective teeth to oversee these issues. This is more fully explored in Chapter 7, Regulation.

Chapter 4 – NSCS for England and Wales – local authorities

The local authorities' strand of the Strategy is led by Tony Gleason, Chair of the Public CCTV Managers Association. Local authorities provide the majority of service provision of State-owned VSS in society. The existence of CCTV operation/control rooms is the legacy of the explosion in the use of such cameras in the 1990s.

Many local authorities work closely with their local police forces that rely on the video they capture as evidence in prosecutions. In addition, operators will often have access to police radio so they can communicate with officers as incidents occur. Elsewhere, there will be agreements in place where the police can access certain CCTV feeds – for example when there are large events taking place. The relationships between local authorities and the police are extremely important with regard to keeping our communities safe.

Service level agreements

In previous annual reports I have been quite candid in my assertation that relationships between some police forces and local authorities are strained. The police have not always been good at providing CCTV managers at local authorities with feedback on the value of CCTV. If managers can't provide evidence that their systems are effective, why should they be kept? This is the question some local authorities are asking themselves and we are seeing local authority CCTV systems being turned off, operating reduced hours or with less staff.

A key deliverable for this work strand is the creation of an SLA framework. It is designed to be used to help police forces and local authorities set up their own SLAs. Tony and ACC Jenny Gilmer are working jointly on this deliverable and enlisting help from others, such as NASCAM and the London CCTV Managers group, to get the broadest input possible to this work.

It is important that such agreements exist as the vast majority of footage from local authority CCTV is ultimately used by the police in investigations – from minor offences to the most serious of crimes. In addition, many local authorities work closely with forces when they are responding to live incidents, for example directing officers on the ground.

Ensuring there are proper, robust and efficient agreements in place are extremely important. However, for something of this nature, where there could be numerous variables between each local authority as well as between each police force, a 'one size fits all' SLA is not the right approach. What is right for one local authority and police force may not be right for another.

What is in development is a template that is simply filled in by both parties, which provides a framework to cover the areas included in any good SLA. These areas include purpose and legitimacy, legal considerations, governance, information sharing, communication, training, surveillance types (overt and covert), finance, feedback, future technology and evaluation/review. The list is not exhaustive and some areas may not need to be used in an agreement. The point is to develop better partnership working that help local authorities and police forces work more effectively in their roles. There is also a role in these relationships for Police and Crime Commissioners who may be able to assist with funding issues if the value of CCTV can be effectively demonstrated.

Properly funded and managed local authority CCTV systems are an essential tool for the prevention and detection of crime and public safety. Robust SLAs can help put in place measures that mean local authorities can effectively evidence the value of that CCTV. The SLA framework should be available in the first half of 2020.

Senior responsible officers and single points of contact

Many local authorities will operate numerous surveillance cameras systems not just a town centre CCTV scheme, and where an authority has no town centre scheme they are likely to have other surveillance camera systems in operation. These could be in libraries, municipal buildings or leisure centres, body-worn video on enforcement officers, AFR systems, ANPR in car parks or traffic enforcement cameras. In all these cases, local authorities must ensure that all CCTV VSS that are operated by the local authority, or on their behalf, are compliant with PoFA and pay due regard to the SC Code. Moreover, all surveillance camera systems will be processing personal data so must be compliant with DPA and the requirements under the General Data Protection Regulation (GDPR).

Local authorities need to maintain the confidence of the public that all the surveillance cameras they operate are used effectively, proportionately and transparently. This can be achieved through compliance with PoFA and DPA/GDPR and by ensuring the local authorities have the correct governance and policies in place.

It is becoming increasingly evident to me that as the technological nature and use of overt surveillance cameras in public places by local authorities continues to evolve then so does the need for the public, and indeed local authorities, to remain both informed and confident as to the legitimacy of those endeavours.

In the reporting year, I wrote to all local authority Chief Executives in England and Wales requesting they identify an SRO to deliver a corporate approach to their responsibilities arising from PoFA. The SRO has strategic responsibility for the integrity and efficacy of the processes in place within the local authority, which ensure compliance with section 33(1) PoFA in support of the Chief Executive, and in respect of all relevant surveillance camera systems operated by the local authority.

I am pleased to report that to date approximately 95% of local authorities now have an SRO in place. This aligns with police forces putting in place similar arrangements and it is at this strategic level where I expect SLAs to be signed and relationships built. Where the SC Code or legislation has not been complied with, my office often finds that it is due to little or no senior strategic oversight within an organisation.

That is not to say that there is an operational failure. Some local authorities are already leading the way at an operational level and have put in place a single point of contact (SPOC) for all matters in relation to surveillance cameras – this is often the town centre CCTV Manager and someone who supports the SRO regarding compliance with PoFA across all the authority's video surveillance schemes. I issued updated guidance in May 2019.[21]

I will be writing to all local authorities again in early 2020 to conduct a survey to identify the nature of the surveillance camera systems which they operate within the scope of PoFA and whether they comply with the provisions of section 33(1) PoFA. I will be reporting findings in my Annual Report next year.

CCTV in taxis

The requirement by some local authorities for taxi drivers to have CCTV installed in their vehicles as part of licencing requirements is an area that continues to be raised with me. I responded to the Department for Transport consultation regarding guidance for taxi and private hire vehicles in April 2019.[22]

The SC Code states:

> "When a relevant authority has licencing functions and considers the use of surveillance camera systems as part of the conditions attached to a licence or certificate, it must in particular have regard to guiding principle one in this Code. Any proposed imposition of a blanket requirement to attach surveillance camera conditions as part of the conditions attached to a licence or certificate is likely to give rise to concerns about the proportionality of such an approach and will require an appropriately strong justification and must be kept under regular review."

Typically, CCTV installed in taxis record audio so the level of intrusion is greater than if only video is recorded. Furthermore, I have had complaints from drivers who state they are unable to turn off the cameras when they are using vehicles for their own private journeys. This is unacceptable. With the introduction of SROs and SPOCs, I am hopeful that where authorities are considering the introduction of CCTV in taxis as part of licencing requirements, that it is done so in line with PoFA and the SC Code.

[21] https://www.gov.uk/government/publications/introducing-a-single-point-of-contact-guidance-for-local-authorities
[22] https://www.gov.uk/government/publications/surveillance-camera-commissoner-response-to-the-department-for-transport-consultation-on-taxis

Chapter 5 – NSCS for England and Wales – voluntary adopters

The Secretary of State's SC Code and the supporting NSCS provide a holistic 'whole system' approach for the management of VSS. I continue to focus on all organisations using such equipment in the public domain because 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]."

The voluntary adopters strand of the Strategy is led by Mike Lees (Head of Business Security, Barnsley Hospital NHS Foundation Trust). Barnsley Hospital was one of the first voluntary adopters to attain my certification mark and Mike is one of the biggest advocates of the SC Code. This strand is broad and challenging as it covers all organisations which are not police forces or local authorities. Mike has recently recruited a colleague from the National Association of Healthcare Security (NAHS) to help him drive up voluntary adoption of the Code – Martin Lomas (Head of Security, Engie).

Over the reporting period we have seen organisations who sit outside the list of relevant authorities in PoFA get my certification mark; for example, the Tower Bridge exhibition became the first certified entertainment organisation. I continue to see regular interest from all types of organisations – the Church of England, Transport for London, Police Scotland, Network Rail, the Police Service of Northern Ireland and Arsenal Football Club are just some of those we have been liaising with.

It is in the parking sector where we have made most progress, often where a range of different types of surveillance cameras are used. I reported last year that we were working with both the British Parking Association (BPA) and the International Parking Community (IPC). The BPA is the largest and most established professional association representing parking in the UK. They have made it a requirement for members of their Approved Operator Scheme to comply with the SC Code. Consequently, 26 BPA organisations have completed the self-assessment tool (SAT) and signed up to the SC Code. Head of Business Operations Steve Clark and Customer Services Manager Gemma Dorans have led the drive to improve compliance via newsletters, online and through engagement with their operators.

In May 2019, my team organised a certification workshop for BPA-approved operators. It was attended by 16 parking organisations and the aim of the workshop was to promote my third-party certification scheme. There were sessions on barriers to certification, a case study, question and answer session, and surveillance cameras and GDPR for added value. Since the workshop, four BPA members have achieved certification and many members have booked audits or made significant progress towards certification. We will be delivering another workshop for the BPA this year.

The IPC represents public and private sector parking operators. The IPC attach a lot of importance to compliance and Membership and Operations Manager Chris Naylor has been leading the process of getting all their Approved Operator Scheme members to complete my SAT and adopt the SC Code. To date, 34 IPC members have completed the tool and adopted the SC Code.

Like with the BPA, we held a certification workshop for IPC members – this was in October 2019. The workshop was attended by 35 people from various parking organisations. Since the workshop, two IPC members have achieved certification and five members are currently working with auditors to achieve certification.

As I have said in previous annual reports, driving up voluntary adoption is one of the biggest challenges I face. Why would an organisation adopt the SC Code when they are not legally required to? That is a question I am often asked and I ask myself. I reiterate 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.

Chapter 6: NSCS for England and Wales – human rights, technology and data

This strand was launched in 2018 with the aim of foregrounding human rights and civil liberties standards into the use of surveillance camera technologies for the provision of public safety. It is led by Professor Pete Fussey, Director at CRISP and Professor in Criminology at the University of Essex.

The strand is designed to operate in dialogue with other strands of the NSCS. The work of other strands will inform the development of this strand. For example, insights from the Horizon Scanning strand will inform thinking over the human rights considerations relating to emerging surveillance technologies. At the same time, the Human Rights, Technology and Data strand will also feed into other areas of the National Strategy, for example through the development of training standards.

The strand has been divided into four areas of work and these are set out below along with commentary on progress made against each deliverable.

Deliverable 1 – Establish human rights subgroup under SCC advisory panel to access a range of perspectives on issues of law, operations and technology

This deliverable is focused on establishing an advisory panel of experts in the theory and practice of surveillance alongside the social, ethical and human rights implications of such uses. This deliverable has been accomplished.

At present, the advisory panel consists of a mix of police, surveillance practitioners, legal experts and civil society groups. Current membership includes: Jenny Gilmer (NPCC Lead for CCTV), Simon McKay (Barrister specialising in surveillance law), Hannah Couchman (Liberty), Anne Russell (ICO), Daragh Murray (Senior Lecturer in Human Rights) and Mick Kelly (SCC Office). This has enabled a wide body of expertise covering operational uses of surveillance and its ethical and human rights implications to become integrated into the work of my office.

Membership is under periodic review and Pete will seek to extend the panel during 2020 to include representation from State agencies using covert surveillance methods, senior members of police ethics oversight panels, a biometrics expert and representation from the Centre for Digital Ethics and Innovation (CDEI), part of the Department for Digital, Culture, Media and Sport (DDCMS).

Deliverable 2 – Scope-relevant existing advice and provision on human rights and liberties in domains that are related yet external to the SCC remit

This deliverable is focused on drawing insights from similar, often parallel conversations happening elsewhere, particularly among other regulators, oversight bodies, ethics panels, policy communities and academics. To achieve this, Pete has engaged with a large number of regulators and institutions in the UK, EU and US. These have included:

- representatives from NPCC;
- The European Union Agency for Fundamental Rights;
- The United Nations Office of the High Commissioner for Human Rights;
- representatives from the DDCMS CDEI;
- parliamentarians;
- both co-directors of the national Independent Digital Ethics in Policing Panel;
- Digital Policing Leads at two UK regional police forces;
- representatives from oversight panels for a further two UK regional police forces;
- Office of the Inspector General for the NYPD;
- representatives from three corporations considered market leaders in the development of digital surveillance technology;
- insights from engagements with IPCO;
- insights from long-term research on digital policing within a major US urban police force;
- UK-based civil society organisations.

Whilst public opinion is not decisive when considering human rights implications, it remains important to the debate, particularly as it relates to increasingly complex considerations around consent in an era of digitally-mediated surveillance. To address this, the deliverable has also encompassed a focus on public opinion and media discourse. This has involved capturing the latest polling data on surveillance acceptability, interviews with journalists, and tracking of social and traditional media.

Some of the themes raised through dialogue with these bodies include:

- **Innovation in surveillance technologies has started to raise a number of rights and ethics-based regulatory challenges.** These include the application of new technologies with potential for surveillance that was unanticipated at the time of legislation. In addition, new technologies are increasingly designed to be both 'repurposable' and interoperable with other systems and data architectures. This may mean surveillance practices may not fit easily into existing regulatory mandates. This may require reconsideration over existing regulatory parameters. In addition, increasing capacities for surveillance systems to interconnect with each other raise further challenges for oversight and regulation. Interoperability necessarily heightens the potency of surveillance measures. Additionally, such practices have implications for 'surveillance by consent', particularly when the subjects of these practices have a reduced opportunity to foresee (and thus consent to) downstream uses of information.

- It is becoming increasingly important to find ways of **anticipating the use and impact of new technologies**. Developments in surveillance equipment make effective regulation more important than ever before. Yet the complexity of this technology makes these forms of oversight increasingly challenging. Closer integration between the Human Rights, Technology and Data and the Horizon Scanning strands of the NSCS is one first step towards addressing this, although this could provide a basis for a more integrated approach in the future.

- As surveillance capabilities develop, **the boundaries between categories of surveillance practices may become blurred**. This is despite the distinction between such surveillance activities for the purposes of regulation and law. These potential ambiguities particularly apply to distinctions between covert and overt activities and, separately, the demarcation between biometrics and other forms of surveillance.

- So far, the analysis has revealed a need to place attention on the activities of surveillance users **prior to the introduction of technology**. Much recent debate has focused on the regulatory coverage of emerging technologies, but less attention is given at pre-controversy/pre-deployment stages. Particular opportunities exist here to encourage responsible decision-making and actively pre-empt likely controversies following deployment. There appear to be two relatively straightforward interventions that can be made here:

    - First is to establish a process of notification regarding the use of particularly controversial technologies. If users were to notify regulators of the intention to deploy, this would immediately confer dividends in terms of transparence, provide a mechanism for accountability and

offer an opportunity to hold constructive discussions over the responsible use of these technologies before any problems may arise.

    - Secondly, and relatedly, attention is needed on the role of pro-active decision-making (rather than post hoc retrofitting of regulatory guidance). Particularly important are mechanisms for embedding human rights concerns at the outset of such processes. This should extend beyond data protection impact assessments to consider the range of rights affected.

- Recent years have seen a growth in **surveillance-related judgments** by the European Courts and this trend looks set to increase (notwithstanding judicial arrangements following Brexit). These activities generate an opportunity to inform regulatory practice by gaining further clarity concerning judicial outcomes and how principles can be read across from court judgments to this space. This indicates the importance of exploring potential synergies from the courts and regulatory policy. At the same time there has been an increase in guidance issued by different State and transnational governance bodies, regulators and civil society groups. Whilst not binding, the analysis of these initiatives can offer useful assistance and capitalise on parallel conversations and expertise exercised in related areas.

- There is an emerging issue of **governance** that, extrapolating from recent trends, is set to gain further relevance in the coming years: the relationships between public bodies and private users of surveillance technology. The current arrangement whereby public and private agencies collaborate in the surveillance of privately-owned yet legally designated public space is problematic. This is because the intensity of regulatory scrutiny falls unevenly across these different actors despite their joint enterprise. Therefore, attention needs to be placed on linkages between public and private space, and on public and private uses of these technologies.

Whilst this deliverable is nearing completion, further engagements are planned during 2020 to capture the most recent developments and debates in this area.

Deliverable 3 – Develop a strategy to capture and communicate core principles concerning human rights as they apply to surveillance cameras

This deliverable is in progress and the intention is to unite insights gained from deliverables one and two in addition to drawing on source material from academic research and current legal and policy debates. The principles will be targeted towards the other SCC Strategy strand leads with the intention of further communication to the public, surveillance camera users, other regulators and relevant government strategy areas.

Deliverable 4 – Integrate Human Rights, Technology and Data strand work with SCC policy developments and other strand activities

This will follow from Deliverable 3. Work will be focused on informing future editions of the SCC National Strategy, SC Code and other instruments with core human rights principles drawn from this strand. Work on this deliverable is in progress and ongoing. Connections have been made with the Civic Engagement strand through secured funding for a co-hosted event in early 2020. This is designed to engage the public over the ongoing dialogue concerning human rights standards and surveillance technology in relation to biometric surveillance. The aims of the Regulation and Policing strands also overlap with the Human Rights, Technology and Data strand in a number of key areas. To foster these connections, the lead of the Regulation and Policing strands participates in the expert advisory panel for the Human Rights, Ethics and Technology strand (Deliverable 1).

For 2020, other planned integration activities include engagement with these strands:

- Horizon Scanning – to ensure currency and that Human Rights strand work is equipped to address relevant and emerging challenges.
- Local Authorities – to scope out and anticipate issues of implementation though engagement with surveillance users.
- Training – to explore opportunities for integrating strand work into training provision and the development of training material specific to human rights on existing courses and bespoke briefings.

Chapter 7 – NSCS for England and Wales – regulation

As I have said throughout this report, it is time that a fundamental rethink is given to how surveillance cameras operated overtly in public places are regulated and the context against which the future role of the SCC should be considered is as follows:

- The technological surveillance capabilities of systems which are operated and integrated with surveillance cameras in public places will continue to evolve and become ever more intrusive upon the fundamental freedoms of citizens either by themselves or where operated in concert with other modalities.
- The propensity for the police and agents of the State to make use of such technologies, many of which are becoming increasingly part of our everyday lives, will increase and the medium by which systems are deployed will similarly evolve (e.g. Google glasses, drones etc).
- Citizens and indeed operators of systems will require confidence that the use of such surveillance capabilities are enshrined in sufficiency of law, guided by clear and transparent codes of practice, and subject to effective and robust regulation.

In a speech I made in March 2018 to the Taylor Wessing Annual Data Privacy Conference I said:

> "I made it clear in my recent Annual Report that I believe the current regulatory framework is not fit to manage the challenges emerging from new surveillance technologies in society. My role has increasingly drawn me through the camera lenses and in to the back office of artificial intelligence and integrated systems over the preceding five years."

That sentiment still rings true now.

Surveillance cameras or surveillance technologies

The unequivocal regulatory focus of my role is the operation of overt surveillance camera systems in public places in England and Wales. It is inescapable that the growing capabilities of technologies to overtly track (i.e. conduct surveillance upon) citizens are matters of increasing public interest and understandable disquiet.

Section 29(6) PoFA defines a 'surveillance camera system' for the purposes of the Act as follows:

> (a) closed circuit television or ANPR systems,

(b) any other systems for recording or viewing visual images for surveillance purposes,

(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or

(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

Sections 6(c) and 6(d) are capable of application to a very wide range of technologies and, whereas 6(b) relates to 'visual images' only, section 6(d) is capable of incorporating audio technologies within its broad definition. A longer-range strategic view of my role may consider whether regulation of 'surveillance cameras' is sufficient for an increasingly technological surveillance society. It is the broader application of overt surveillance technologies which may occupy a gap in regulation, whether those surveillance modalities will be movement sensors and blue tooth technologies, or cameras which combine biometric and/or open source information.

A longer vision of such matters may therefore question whether my role should evolve to a broader role of Overt Surveillance Commissioner with the potential to merge functions and back office resources with the Biometrics Commissioner, or indeed more reasonably become an additional function sitting within the framework of the Investigatory Powers Commissioner. This latter option would have the benefit of having the regulation of state surveillance in all its forms sitting within a single Commission supported by legal provision and an inspection function.

Effective regulation

The capabilities of overt surveillance camera technologies are developing to the point that they are arguably at least as intrusive as some covert law enforcement techniques which require authorisation under the terms of RIPA. The effective regulation of the operation of overt surveillance camera systems will necessarily require:

- A clear and consistent understanding by all parties as to the legal basis upon which the police and relevant authorities rely for the conduct of surveillance by means of an overt surveillance camera system.
- An up-to-date and relevant SC Code supported by regulatory guidance where necessary.
- The ability to provide intrusive and robust regulatory scrutiny and thereby influence the use of technologies.
- A re-appraisal as to the adequacy of the scope of relevant authorities bound by any revised code.

Surveillance vs. data protection

Surveillance is an investigatory power and, when conducted by agents of the State, draws on a wide range of supporting legislative considerations. Surveillance, whether overt or covert in nature, engages a range of citizen's fundamental freedoms and therefore may require a legal basis for its conduct. Within the domain of covert surveillance, RIPA provides such a legal basis where surveillance is either 'directed' or 'intrusive' in nature. When surveillance is conducted 'overtly', common law and PoFA have bearing.

DPA applies equally to covert and overt surveillance in terms of regulating the processing of personal data, and unquestionably provides significant and enhanced responsibilities and controls to the processing of personal data. It is asserted by commentators such as Liberty, Big Brother Watch and indeed the SCC that this legislation does not provide a basis in law for the conduct of surveillance by means of overt surveillance camera systems in the same manner that RIPA does so in terms of covert surveillance.

Surveillance material – the product derived from a surveillance camera – may be evidence, intelligence, information, data and personal data, and, when considered alongside the 'surveillance conduct' undertaken by agents of the State, arguably engages a broad range of statutory and regulatory considerations of which DPA is but one.

Of course, everything is data. However, the very essence of surveillance by the State is a far broader and deeper consideration than data protection requiring a specific and specialised regulatory focus. It was that very recognition which resulted in the creation of my role. Indeed, such recognition has similarities with ministers' recognition that social media and big data issues would benefit from a new and bespoke regulatory role, beyond that of data protection alone.

It is significant that the consultative approach in Scotland to considering the future regulation of biometric technologies delineates data protection considerations.

A harmonious approach towards a future paradigm which revises and refreshes the regulation of state surveillance within a single commissioning body, acting in harmony with the ICO may be an attractive proposition.

To consider amalgamating my functions within the ICO would be to split the regulation of overt and covert surveillance by the State between two bodies leading to differing standards, requirements and approaches. Overt surveillance camera systems can and regularly are used to conduct covert surveillance. The potential for overlap and confusion are therefore obvious.

Surveillance Camera Commissioner

My role and functions were created by virtue of section 34 PoFA. Since inception, the role has evolved considerably to become a leading regulatory voice in the field of the operation of surveillance camera systems in public spaces in England and Wales. There are many successes which may be directly attributable to this role. My role is subject to periodic review and the following observations are offered in respect of the role:

- I have no powers of inspection, audit or sanction.
- I am increasingly required to provide commentary on legal issues that predominantly arise from the complexities associated with balancing the use of modern and advancing technologies against current legislation and an increasingly out-of-date code of practice. I have no ready recourse to independent legal advice.
- There is some evidence arising from the verbal submissions to the Home Affairs Science and Technology Committee that the Home Office erroneously regards the regulation of overt surveillance camera technologies such as AFR only through the prism of data protection legislation.
- The media, the public and the stakeholder community have an increasing appetite for information and leadership in respect of the subject matter.
- The demands on my office regularly outstrip the ability of resources to deliver, so strict prioritising is required.
- The demands placed upon me necessitate me working beyond my limited contracted dates.

The future…

Whereas the consideration and delivery of a new paradigm for the regulation of overt State surveillance may be an attractive option for some, in reality such an approach would potentially impact upon precious Home Office and Parliamentary time which will be very much at a premium over the coming years, and therefore a shorter-term evolutionary option may have greater relevance.

The majority of themes contained within PoFA arguably lend themselves more towards security than data identity – pre-charge detention of terrorism suspects, additional requirements placed on local authorities conducting directed surveillance and deploying covert human intelligence sources (CHIS) – and therefore the responsibility for future iterations of the SC Code may sit more comfortably with the expertise within the Office for Security and Counter Terrorism (OSCT) within the Home Office rather than the Data and Identity Directorate.

My functions and that of my support team may be better served within the structures of IPCO. The following considerations may apply in such an approach:

- Overt surveillance camera systems are often operated to conduct covert surveillance (e.g. local authority CCTV) so both of the Home Secretary's surveillance-related codes may be relevant in given circumstances. In any event a consistency of language and content/underpinning guidance would remove any potential for confusion.

- The majority of 'relevant authorities', as described by PoFA, who must have regard to the SC Code are also prescribed as 'public authorities' who are enshrined with the powers and responsibilities associated with the conduct of covert surveillance by virtue of RIPA.

- The IPCO inspection regime can, if minded to do so, test police and local authority compliance with the SC Code simply by scrutinising the approach of a public authority in England and Wales to the provisions of paragraphs 3.36, 3.37 and 3.38 of the Code of Practice for Covert Surveillance and Property Interference issued under the provisions of RIPA. Aligning the SCC with IPCO together with his resources may enable a degree of scrutiny of SC Code compliance as a matter of process.

- IPCO have a legal section which is skilled in matters relevant to surveillance conducted by agents of the State.

Of course, a combination of existing responsibilities, demands and resources would understandably give rise to reluctance for IPCO to take on additional responsibilities; however, if my team and I simply sit within IPCO, the reallocation of existing resources should be comfortably manageable.

I also understand that to have overt and covert surveillance regulated by one Commissioner may be presentationally difficult for the Government if it is perceived that all surveillance is covert or secret. As mentioned above, overt cameras are used covertly so there is already overlap. If there are concerns an organisational design model could be achieved where the SCC works under the IPC with distinct responsibility for overt surveillance and separations in place where necessary to prevent conflicts of interest. This can be communicated in such a way that stakeholders and the public understand the splits.

The Surveillance Camera Code of Practice

The SC Code is the regulatory leadership code of practice for operators of surveillance camera systems which sets the Secretary of State's standard for camera operators. It is a good document and forward looking in terms of future technologies and good practice, and in signposting other statutory and good practice considerations, is considered as a 'leadership piece' of regulation. It has over the

years been allowed to diminish, but in reality its current content simply needs updating and adding to (rather than taking away from). In that respect it should not be an overly challenging or time-consuming undertaking to deliver an updated and credible revised SC Code and one which provides a consistency of language and approach to the regulation of surveillance elsewhere within the Home Office.

'Surveillance' as a theme is fractured within the Home Office between Home Office Policy and OSCT. The Home Secretary delivers two principle codes of practice relevant to both covert and overt surveillance and under the provisions of two separate statutes. Common sense alone would suggest that there should be a consistency of approach and language within these codes to aid those who are regulated by them, as well as informing the public who would want confidence in them.

No change

The challenges posed to society arising from the use of surveillance camera systems have evolved considerably since the inception of PoFA and the role of the SCC since 2012. In the intervening period, such have been the challenges associated with the regulation of state surveillance that new and significant legislation has been passed, regulatory bodies such as the Office of Surveillance Camera Commissioners, Interception of Communications Commissioners and the Intelligence Service Commissioners have been abolished and replaced by IPCO. A new DPA and the GDPR have been introduced, and the ICO significantly empowered and emboldened by growth in numbers. The regulation of overt surveillance camera systems, however, remains entrenched in 2012 requiring a part-time Commissioner supported by three members of staff and no powers or legal support to carry the public interest, delivering a National Strategy led by experts in the field on a 'pro bono' basis.

Whereas major surgery may be a long-term luxury in terms of strategic change, it would make sense to at least have the debate in the short term, recognising that little more than 'kicking the can down the street' is the best that can be achieved in the short term.

A review…

Linking this back to advancing technology, voices from within Government as well as those outside have been calling for a public debate on the use of AFR. In support of those voices, I would go a step further and say that we need an independent review commissioned and conducted of the statutory and regulatory framework which governs the investigatory power of overt surveillance camera use by the State.

The growing capabilities of overt surveillance technologies, the proliferation of cameras in society, the increasingly crowded regulatory space and the voices of concern are such that these matters are increasingly 'a question of trust' for society.

If I have learned one thing from my experience within the NSCS, it is that the framework which delivered my role and the rules by which overt state surveillance is conducted has to evolve and be future-proofed by being principle-based. The days of fragmenting the regulation of state surveillance on the basis of whether a camera is being used ‘covertly’ or ‘overtly’ are gone in my view.

I simply posit the view that some overt surveillance camera applications, whether in themselves or combined with other technologies, are so progressively intrusive in their capabilities that they can be the equal of some covert surveillance activities in terms of the intrusion caused. I believe that it is time the Government recognised overt State surveillance as being an investigatory power rather than simply a data protection issue. An informed and esteemed independent reviewer would I am sure provide such clarity as to the way forwards.

Implicitly my role is to raise the standards of public surveillance operation; to ensure that the public are better informed, more confident and safer; to ensure that the State is clear and accountable for acting within legal and ethical boundaries; that stakeholders and industry have clarity in leadership and standards; and to help inform the evolution of laws and regulation that contribute to keeping us both safe and free.

Regulators working together

Regardless of the direction that the Government choose to take in this area, one thing is clear – where there is regulatory overlap, regulators must work together to provide clear guidance for those deploying surveillance cameras and members of the public alike. This is a key aim of the National Strategy and will continue to be as we move into the 2020s.

Annex A: Surveillance Camera Commissioner's Office resourcing/budget

This table sets out resourcing for the office of the Surveillance Camera Commissioner (SCC) – a rationale for these roles is set out later in this Annex. Note that the SCC team is small and dynamic so there will be fluidity with the roles. The roles below and rationale later in the document are ambitious but they reflect the work of the Commissioner over the past six years and the direction the role is likely to take in the future given emerging surveillance camera technology.

Role	Civil Service Grade	Responsibilities
Chief of Staff (new role)	G6 (F/T)	• Management of the Commissioner's Office including budgets • Strategic oversight of the National Surveillance Camera Strategy (NSCS) for England and Wales working with Commissioner to set strategic direction • Management and liaison with senior level stakeholders at a national level – chief constables, chief executives, National Police Chiefs' Council (NPCC) leads, Police and Crime Commissioners (PCCs), senior academics, senior Home Office and other senior Government officials and regulators etc • Deputising for the Commissioner at strategic board level meetings • Deputising for the Commissioner at speaking events (if appropriate)
Head of Policy	G7 (F/T)	• Strategic oversight of SCC policy and policy development • Overseeing drafting policy documents – e.g. manuals of guidance that accompany SC Code • Overseeing drafting bespoke guidance for relevant authorities such as automatic facial recognition (AFR) guidance, guidance on partnership working etc • Working with partners on joint guidance e.g. Information Commissioner's Office (ICO), Local Government Association, NPCC • Support Commissioner in drafting Annual Report • Thematic research into emerging policy areas that are relevant and horizon scanning

Role	Civil Service Grade	Responsibilities
		• Policy liaison with Home Office, Othe Government Departments and others
Communications Manager (new role)	SIO (F/T)	• Development and maintenance of strategic communication strategy • Oversight of all communication channels – website, social media, blog events, press etc • Advising the Commissioner on press and speaking at events including drafting speeches • Drafting content for communications channels • Management of marketing/communications budget • Devising communications plans for specific deliverables in the NSCS e.g. Surveillance Camera Day, launch of new products etc • Identify innovative opportunities for communications including digital media • Media monitoring and reporting • Manage branding e.g. for new certification schemes

Operations Manager	SEO (F/T)	• Management of SCC certification schemes:
		  ○ Third-party certification – 85 certified organisations (reviewed annually)
		  ○ Secure by Default for manufacturers – self-certification scheme
		  ○ Installers certification scheme – launching May 2020
		  ○ CCTV monitoring centre scheme – launching May 2020
		  ○ Secure by Default for installers – launching 2020 (TBC)
		  ○ Secure by Default for manufacturers part two – launching 2021 (TBC)
		• Encouraging adoption of certification schemes working with relevant National Surveillance Camera Strategy (NSCS) strand leads (local authorities, police and voluntary adopters) and Communications Manager – this includes identifying case studies
		• Liaison with certification bodies
		• Single point of contact for queries from organisations who have been certified or are seeking certification
		• Responsible for Freedom of Information and Data Protection Act (DPA) issues for Commissioner

NSCS Project Manager	HEO (F/T)	• Project manage the NSCS • Work with strand leads to ensure they are supported in meeting deliverables – include regular meetings

Role	Civil Service Grade	Responsibilities
		• Attend strand lead working groups to represent Commissioner and ensure work fits with strategic direction of the Strategy • Manage risk grids and other key documentation • Oversee periodic refresh of NSCS
Administrative Support Officer	EO (F/T)	• General administrative support • Managing diaries • Managing correspondence • Managing SCC inbox • Filing • Booking rooms and organising meetings • Minute taking • Horizon scanning • Manage team action log and team meetings
Data protection expert (new role)	Secondment from ICO (F/T)	• In-house data protection expertise to provide support to Commissioner and liaison point with ICO at a working level. This role would not provide advice on personal data we hold but input into products, policy, guidance that we issue
Legal support (new role)	SEO equivalent (P/T)	• In-house legal support

All the roles outlined above reflect how the SCC has developed in the past six years, including how the volume of work has increased and the need to manage that work effectively. The resource and budget has remained static over that six-year period.

Chief of Staff – G6

The Commissioner and his office require a senior leader to credibly represent the Commissioner. On the basis that this person will be working with numerous external stakeholders of a very senior nature e.g. chief constables, chief executives, NPCC leads, PCCs, senior academics, senior Home Office and other senior Government officials and regulators, it is anticipated that this role would be G6 and they would also act as a deputy for the Commissioner and manage the office.

Head of Policy – G7

This role reflects the volume of policy issues that the office deal with, ranging from general CCTV-related issues to complex issues involving AFR, and connected and integrated technologies. This role would include oversight of policy guidance that sits alongside the SC Code as well as assisting the Commissioner in drafting his Annual Report to Parliament. They would also be required to horizon scan and bring emerging policy issues to the attention of the Commissioner and relevant policy teams in Home Office and wider Government.

Communications Manager – SIO

This role was in an earlier team structure and should be reinstated. The Commissioner requires a communications expert to manage his various communication channels, act as first point of contact press, draft content and develop communications plans and strategies. The Commissioner is contacted on a daily basis for comment on issues by media and this needs to be managed. Also, given the outward facing nature of the Commissioner's role, there is a need for expert communications advice and liaison with other communications experts in other organisations. With new certification schemes imminent, communications will step up over the next 12 months and beyond, and these need to be managed by a communications expert as opposed to policy officials which is the current situation.

Operations Manager – SEO

The Commissioner now oversees a number of what could be described as 'operational' functions. These are essentially the Commissioner's certification schemes – we currently have 85 organisations that have our third-party certification mark (these are renewed annually). We anticipate all 400+ local authorities and all 43 police authorities moving towards certification in the next 18 months. We are also targeting other sectors – NHS, the Church of England, parking and retail, which will further increase demand in this area. In addition,

alongside this we have launched Secure by Default for manufacturers and we are launching new schemes in 2020 which will need to be managed.

NSCS Project Manager – HEO

The NSCS contains 12 work strands, each lead by a sector expert and containing four or five deliverables. The Strategy needs careful project management to ensure strand leads are supported and are on track to meet their deliverables. The NSCS is also coming to the end of its initial phase (2017-2020) and needs to be refreshed, which will require close working with the Commissioner and other strand leads.

Administrative Support Officer – EO

This role is administrative for the Commissioner and rest of the team.

Data protection expert – secondment from ICO

The Commissioner's work is extrinsically intertwined with data protection-related issues which come up on a daily basis. There is currently no expertise within the team to deal with all of these satisfactorily and we refer many straight to the ICO. We also require data protection input into the many pieces of guidance and policy we develop and publish – this is currently achieved by working with officials in the ICO but can be time consuming. This requirement is likely to increase as we enter a world of interconnected surveillance, AFR and other biometric-related surveillance camera platforms. A data protection expert embedded in the team on secondment from the ICO would help alleviate pressure in this area.

Legal expertise

The recent High Court case on AFR has highlighted a resource gap with the Commissioner's office with regard to legal expertise. Additionally, there are occasions where the Commissioner requires legal advice but cannot (understandably) obtain this from HOLA solicitors (Home Office Legal Advisory). Legal advice is not a continued resource requirement so it is proposed that the Commissioner can have access to a solicitor for legal advice. This could be a shared resource for the Biometrics Commissioner and Forensic Science Regulator.

Other budgetary considerations

Consideration should be given to a specific marketing budget – this would be used for communications around Surveillance Camera Day, launch of certification schemes, workshops etc. Ultimately, we would evaluate such a budget against driving up standards amongst surveillance camera operators, installers and manufacturers. This would need to be determined with Home Office Communications but we estimate £50k.

Consideration should be given to funds outside of the Commissioner's budget envelope regarding engaging the Government Legal Department (GLD) and other legal advisors, specifically, when thinking about significant costs such as we have seen through the recent High Court case. Funding such endeavours within budget will inevitably mean we overspend, so a legal fund seems sensible. Would suggest a minimum of £50k based on legal spend on the Bridges v South Wales Police case.

Annex B

The Overt Operation of Surveillance Camera Systems in Public Places by the Police in England and Wales, section 33 of the Protection of Freedoms Act 2012 (PoFA) and the Surveillance Camera Code of Practice (SC Code). A survey and assessment of police capabilities and compliance conducted by the Surveillance Camera Commissioner (SCC).

Introduction

1. The gaze of surveillance camera systems increasingly pervades many aspects of our daily lives. Whether those cameras are being operated by the police, local authorities, other agents of the State, the private sector or indeed by citizens themselves using smart devices or domestic CCTV. It is inescapable that evolving surveillance technologies and their proliferation in society conspire to yield more about us to others and often in a way that is beyond our immediate control.

2. In the context of surveillance cameras being operated overtly by the police, questions prevail as to the extent to which such surveillance should be allowed to be conducted as a legitimate undertaking in a free society. Whereas the inordinate amount of coverage afforded to the police use of facial recognition technologies has understandably consumed so much attention in recent times it is important not to lose sight of the more central issue. This is the developing use of police overt surveillance capabilities, the efficacy of law and regulation, and the challenges which technologies continue to bring, including of course challenges for the police themselves.

3. It is the long-held view of the SCC that to deny the police the opportunity to exploit technologies to keep us safe – technologies that are in everyday use elsewhere for our convenience – and for commentators to proffer inaccurate observations simply denies the public the opportunity to arrive at a balanced view on such matters, and ultimately risks constraining our police to an analogue law enforcement capability in a digital age. Such constraints and risks are both self-inflicted and counterproductive if the police themselves embark upon surveillance activity which is ill considered, ill governed and illegitimate. The challenge for the police using surveillance camera technologies is to engage and to actively keep the public informed through transparency of endeavour, whilst working ethically and in accordance with both the letter and the spirit of the law.

SCC Survey 2019 (an assessment of police surveillance capabilities and compliance with PoFA and the SC Code).

4. In June 2019, the SCC wrote to the Chief Officers of the 43 police forces in England and Wales and also to the British Transport Police, Civil Nuclear Constabulary and the Ministry of Defence Police. The 46 Chief Officers were invited to complete a simple survey form to account for:

    - the surveillance camera systems that their force operated and which fell within the remit of PoFA, together with the extent to which the operation of those systems complied with that legislation;
    - details of partnerships between their force and third-party system operators; and
    - any good practice they wished to share or further guidance they considered necessary.

5. This process sought to build upon similar undertaking which was conducted by SCC in 2017. This was to understand how the police overt surveillance camera capabilities were evolving and how governance arrangements and statutory compliance of those capabilities were being addressed.

Compliance

6. Compliance is a consistently used term throughout this process. In the context of PoFA it relates to compliance on the part of the relevant authority with the duty to ***have regard*** for the SC Code arising from section 33(1).

7. The guidance of the SCC is that to have 'regard' to the SC Code is to ensure that the operation of a surveillance camera system is demonstrably undertaken in a manner which is wholly compliant with its provisions. Any deviation or derogation from its contents on behalf of a relevant authority should be a decision made by, or on behalf of the Chief Officer by the Senior Responsible Officer (SRO) and recorded by them as a matter of policy. Any policy decision should clearly set out the relevant provisions of the SC Code from which the force derogates together with an explanation for that decision being made.

8. The guidance of the SCC is also that compliance with section 33(1) should be capable of being verifiable by a third party by means of the existence of a suitable record or audit trail which appropriately demonstrates that regard has been given to the SC Code in respect of each system being

operated. To assist relevant authorities, the SCC has produced a self-assessment tool (SAT) to enable them to assess their standards of operation against the provisions of the SC Code and to draft an action plan where they assess that further work is merited by them to meet the provisions of the SC Code.

Outcomes

9. The results of the information provided within this report are necessarily caveated with caution when seeking to draw meaningful conclusions. The 46 Chief Officers engaged by this process were simply asked to provide the information requested in so far as it related to their particular force within the period of time accommodated by the survey window, this being from 20 June to 22 July 2019. In essence, the results of this process are simply a 'snapshot' of the situation which was reported as existing in each force at that particular time and of course things may have changed since then, for better or for worse.

Section A – Governance and categories of systems

Governance

10. By appointing an SRO, a Chief Officer of police may derive additional confidence from a corporate approach being applied to ensure compliance with PoFA and the SC Code in respect of those systems which their force operates. The police are very familiar with the concept of an SRO as such a role is long established within forces in respect of the covert surveillance activities arising from the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA).

11. It was reported that, with one exception, every Chief Officer had appointed an SRO with specific responsibility for ensuring PoFA compliance within their forces. One police force reported that it hadn't made use of any surveillance camera systems within the ambit of PoFA and the SC Code and therefore the Chief Officer had not appointed an SRO. The rank/grade of the SROs as reported were as follows: three Deputy Chief Constables, 16 Assistant Chief Constables, two Commanders, three Chief Superintendents, 13 Superintendents, one Inspector, one Head of Information, one Chief Information Officer, one Head of Information Security and Governance, and one Head of Transformation. One particular force reported that it had appointed three separate SROs internally for differing functionalities – two Chief Superintendents and one Superintendent.

CCTV – internal systems

12. Of the 46 police forces that responded to this category of the survey, 43 reported that they operated internal CCTV systems and 30 (70%) of these were reported as being compliant. In 21 of the 30 cases (70%) reported compliance was demonstrated by means of a SAT. There were eight of the reported systems said to be operated as collaboration with other forces. The reported CCTV systems were located in public counters/help desks and public waiting areas for custody suits. The majority of systems had visual-only capabilities and others had both audio and visual. There was an example of such a system being operated together with the local authority. Three forces reported that they did not operate internal CCTV systems.

13. Thirteen forces reported that their systems were not compliant with PoFA and the SC Code.

CCTV – external systems

14. There were 38 forces reporting that they operated external CCTV systems, of which 28 were reported as being compliant, and 20 (74%) of these systems demonstrated compliance by means of a SAT. The nature of the systems reported tended to be external perimeter security systems and those sited at police car parks. Two forces reported that they owned and operated CCTV systems which were located in local towns.

15. Ten forces reported that their systems were not compliant with PoFA and the SC Code.

16. In the case of both internal and external CCTV systems, the reasons offered by the police for non-compliance included that systems and policies were being subject to review and, in many instances, a SAT provided by the SCC had been completed by the force and had indicated that further work was required to achieve compliance.

ANPR – fixed site

17. Of the 46 forces, 45 reported that they operated a fixed-site ANPR system. There were 24 forces who reported that they operated ANPR in collaboration with other police forces.

18. Of the 45 forces who operate this system, 41 (91%) systems were reported as being operated in compliance with PoFA and the SC Code. In 36 of these cases, compliance was demonstrated by means of a SAT; other examples pointed towards the National ANPR Standards for Policing and Law Enforcement, and local policy and procedures as being appropriate evidence of compliance.

19. Four forces indicated that their system was not compliant. Rationale included internal restructure affecting the ANPR coordinator's function, and recently completed SATs which highlighted further work required to deliver compliance.

ANPR – dashboard mounted

20. There were 39 forces who reported deploying a dashboard mounted ANPR capability and 16 of those forces reported operating their system in collaboration with other police forces. Primarily these systems were operated at the tactical level by specialist policing teams, other road policing teams and armed response vehicles, many with both forward and backward facing cameras. Although this capability was deployed on marked and overt police vehicles, there were examples of unmarked vehicles also being similarly equipped.

21. Six forces reported that their systems were not compliant.

ANPR – other systems

22. There were 14 forces who reported that they operated ANPR systems within this category, five of which said they did so in collaboration with other police forces.

23. These systems were largely those being operated to facilitate temporary deployments at pre-determined locations and were variously described as being 'spike cameras', standalone battery-operated systems. Others were systems installed in safety or 'Spectrum' vans and within a command van facility.

24. All of the 14 'other systems' declared were reported as being compliant with PoFA and the SC Code.

Body-worn video cameras (BWV)

25. Of the 46 forces, 45 reported that they operated BWV. Of those 45 force systems, 42 (93%) were reported as being compliant and in 36 cases,

compliance was reported as being demonstrated by means of a completed SAT. There were 19 forces who reported that their systems were operated as part of collaborative arrangements with other forces. The nature of the systems reported were mainly body-worn devices which were variously allocated to front line patrol, neighbourhood policing/PCSO and other operational functions as the force deemed to be appropriate. Other systems reported were helmet cameras being allocated to armed response officers.

26. All of the BWV systems reported had both audio and visual capabilities operating. One force reported that its system had additional capabilities not currently is use, which were described as being 'stealth mode' wi-fi and live-time streaming. There was one example which indicated that an 'app' was being considered '*for trial in the Autumn which will permit the live-time viewing of footage being recorded between camera and viewing tablet/mobile device in order to comply with Code G changes regarding interviews outside of the custody environment'.* Another example indicated that its system was being upgraded and that there was an intention to make use of it to conduct interviews with suspects arising from changes to Code G of the Police and Criminal Evidence Act 1984.

27. Three forces reported that their BWV systems were not compliant. Each explained that they had completed a SAT and were undertaking action to address any shortfalls identified by the process so as to achieve compliance.

28. It was encouraging to note the high degree of compliance reported (from 67% in 2017 to 93%) amongst an increasingly prevalent capability (from 42 to forces to 45 forces using BWV) and that action was in hand by those forces who said that they did not yet comply.

Unmanned aerial vehicles (UAV/drones)

29. There were 35 forces who reported that they operated camera-borne UAVs and 32 (91%) of those systems were reported as being compliant with PoFA and the SC Code; 23 of those cases demonstrated compliance by means of a SAT. One force reported that it had recently purchased a number of UAVs (number not reported) but had not yet progressed to deploying those resources operationally.

30. Those 35 forces who operated UAVs reported that they had 209 UAVs between them. This number includes the recently purchased but not yet operational capability reported by one force.

31. The capabilities of the UAVs were variously reported as including still and video photography, zoom, thermal imaging, infra-red, low light sight and LED illumination.

32. Of the forces responding to the 2017 SCC Survey, 25 forces (56%) reported that they had a UAV capability of which 14 (56%) were compliant compared with the current position of 35 of the 46 forces (76%) having the capability now with 91% of forces demonstrating compliance.

Helicopter and fixed-wing borne surveillance camera systems

33. The National Police Air Service (NPAS) is the police aviation service that provides centralised air support to all territorial police forces in England and Wales. The lead force for NPAS is West Yorkshire Police. The helicopters and fixed-wing resources carry a variety of video camera capabilities.

34. The systems were reported as fully operating in accordance with PoFA and the SC Code.

Other systems

35. Chief Officers were asked to report upon any other systems which they operated and which they had themselves assessed as being a surveillance camera system which sat within the purview of PoFA and the SC Code. They were then asked to explain whether those systems were being operated in compliance with those provisions.

36. There were 22 police forces who between them reported a further 39 surveillance camera systems which they had identified as being systems to which PoFA and the SC Code applied. Of those 39 systems, 20 (56%) had been assessed as being compliant, and a SAT having been completed in respect of 12 of those systems.

37. There were various capabilities which were reported and were described as follows:
    - Video cameras used by evidence gathering teams at public order events (reported the greatest number of times by forces (eight))
    - In-car media (public order vehicles, unmarked vehicles, marked vehicles and custody vans)
    - Live-time use of automatic facial recognition (AFR) (Metropolitan Police Service and South Wales)

- Dog-borne cameras used for firearm operations
- Cameras attached to bicycle handlebars
- Moveable CCTV systems
- Moveable cameras with laptops
- Cameras deployed to protect vulnerable people

38. There was an inconsistency across forces as to the systems they reported or indeed whether they reported any additional systems as being relevant to the provisions of PoFA / SC Code at all.

Section B – Partnerships

39. Chief Officers were asked to identify and report upon those partnerships which their force had established with third-party operators of surveillance camera systems in the public sector, private sector, with communities in relation to domestic CCTV systems or any other partnership arrangement.

Police partnerships with local authorities / public bodies

40. A total of 42 forces confirmed that such partnerships existed with local authorities. Predominantly these arrangements involved local authority CCTV systems being linked to and viewable by police control room centres. Additionally, arrangements were also reported whereby the police were afforded access to local CCTV systems where necessary to view or recover images / surveillance material.

41. There were examples provided of partnerships with Fire and Rescue Services in respect of the use of UAVs and also with the Coastguard.

42. Four forces reported that they did not have any partnership arrangements with third-party operators of surveillance camera systems in the public sector.

Police partnerships with private sector / commercial / retail bodies

43. There were only 16 of the 46 forces who reported that they engaged in partnerships with private sector bodies in respect of the systems which they operated. The nature of those systems tended to be systems such as CCTV at shopping centres, public transport locations, rail and passenger hubs and football/sporting event locations.

Police partnerships with domestic CCTV systems

44. Only one force reported that it engaged with residents in respect of domestic CCTV systems, albeit on an informal rather than a formal partnership basis.

Other partnerships

45. There were five responses made by forces within this section. The partnerships reported were a combined partnership with local authority and commercial/retail premises regarding CCTV, a partnership with Fire and Rescue Services regarding UAV, partnership with a retail centre regarding use of ANPR, image sharing regarding AFR, and systems relating to the critical national infrastructure.

Partnership summary

46. The completion of this section appeared to cause some forces difficulties as a significant proportion of responses were not completed, were vague or involved an inordinate time delay beyond the assessment process timeline to provide the information requested. The nature of the responses received, particularly with regards partnerships between the police and the private/commercial/retail sector and also residents, are probably unlikely to be an accurate reflection of the extent of partnership activities which exist. A Chief Officer will want to be assured that partnership arrangements are not being established by members of their force without proper management controls being applied. Such controls are important to ensure that a force is not at risk of being vulnerable to legal or reputational damage, either due to the technology concerned, the organisation(s) involved, or the manner in which the surveillance is conducted and the surveillance material used.

Section C – Good practice and guidance

47. The low level of submissions aside, there is evidence of good practice emerging from the activities of some police forces which may be of benefit to others. Of course, there may or may not be other examples elsewhere which simply were not highlighted as part of this process. The NPCC lead for these matters may wish to consider whether it may be helpful to the police to establish mechanisms which will better enable Chief Officers to share and learn from good practice which emerges from the activities of their force when seeking to raise their standards of operating surveillance camera systems in accordance with the provisions of the SC Code and to

further enable closer working with the SCC to consider and promulgate such matters.

48. From the low volume and the content of those responses submitted, there are few meaningful conclusions which may be drawn. There is clearly some appetite from the few forces who addressed this section to learn from good practice elsewhere, hold workshops and work closer with the NPCC leads for surveillance camera systems. Regardless, the inconsistencies in responses to the survey and low level of application to this section serve to indicate that better guidance than that which currently exists, and indeed has existed for some time, would be beneficial to achieving a greater degree of consistency. The SCC has provided guidance in respect of the police use of AFR in the context of PoFA and the SC Code.

Concluding remarks and recommendations

49. In many respects, the results of the SCC Survey 2019 seem to indicate an improved position in terms of compliance by Chief Officers with the provisions of section 33(1) PoFA and the SC Code in respect of the systems which their forces operate.

50. The information provided suggests that there is still room for improvement by many police forces. Clear leadership and firm governance within a force are essential in ensuring that effective coordination at the strategic level translates into equally effective compliance at the operational level. Surveillance camera systems prevent crime and they assist police with the response, command and control, investigation, detection and prosecution of crimes. The integrity and legitimacy of conduct and resulting surveillance material are essential to public trust and confidence as much as they are to delivering a safe society.

51. It is acknowledged that compliance with the legislative provisions of PoFA and the SC Code are matters which compete amongst a huge portfolio of statutory responsibilities for Chief Officers battling growing remorseless demand with finite resources. However, this is not new legislation and its provisions should be familiar to, governed by, and embedded within the activities of a police force to a consistent standard and to a similar extent as those which govern its covert surveillance practices. They are not.

52. The national ANPR system has been upgraded in recent years and is far more prevalent and intrusive in its capabilities than before.

53. There are more BWV cameras being operated by more police forces and with additional applications of their capabilities being considered.

54. There are more forces employing UAVs with more than 200 units owned by forces and they are carrying various surveillance capabilities.

55. There is an inconsistency inherent in forces identifying the systems which they operate which fall within the purview of this legislation.

56. The police use of facial recognition technology is being challenged through the courts.

57. The police conduct surveillance on their communities using surveillance camera systems operated by third parties which are not regulated as state actors, albeit other statutory controls exist. The provisions of PoFA and the SC Code apply to these arrangements. However, the extent to which a force executive is undertaking such activity, with which organisations using which technologies and to what extent, are areas for further consideration in terms of governance.

58. It is of concern that some forces consider a particular system as falling within the purview of PoFA and the SC Code where others do not. Some forces readily can identify the partnership arrangements with third-party operators of systems, others less so.

59. The following recommendations are made:

Recommendation 1 – In the first instance, it is recommended that the Chief Officers and SROs of those forces who as part of the SCC Survey 2019 reported that their surveillance camera systems were not being operated in accordance with section 33(1) PoFA and the SC Code, review their provision to ensure that those systems are operated in accordance with the legislative requirements which apply.

Recommendation 2 – In support of the Chief Officer, SROs should consider whether there are sufficiently robust governance and oversight arrangements across the force (or collaboration of forces) which ensure that partnership arrangements with third-party operators of surveillance camera systems, particularly those systems with additionally intrusive capabilities or otherwise provide a heightened risk of legal or reputational impact, are:

a) readily identifiable by, or notified to, an SRO;
b) conducted in accordance with the law, the SC Code, regulatory guidance and policy;

c) documented in a written protocol (SLA, MoU etc); and
d) there is clear police responsibility and accountability established for the use of a third-party system in partnership.

Recommendation 3 – It is recommended that Chief Officers and SROs 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 Chief Officers to discharge their responsibilities arising from section 33(1). Such processes should:

a) keep the development, procurement and the operation of future systems under review so as to determine and address the inherent legal responsibilities associated with their operation appropriately (*new and future capabilities*);
b) incorporate the partnership arrangements between a police force and third-party operators of surveillance camera systems (*partnerships*);
c) incorporate the efficacy of arrangements between a police force and the Crown Prosecution Service which ensure that any disclosure considerations which arise from the police use of surveillance camera systems in judicial proceedings are properly addressed (*disclosure*);
d) ensure that any intention to trial or pilot a system will in turn ensure that the operation of the system complies with the law (PoFA) and SC Code before, rather than after any trial or pilot is undertaken in a public place (*police trials*);
e) be conducted by the SRO and kept under regular review at intervals no greater than one year (*regular reviews*);
f) be able to facilitate the timely and accurate reporting of information as requested by the SCC which is relevant to the police operation of surveillance camera systems and relevant partnership arrangements which fall within PoFA and the SC Code (*reporting and coordination with regulator*).

CCS0420516330
978-1-5286-1917-2