SURVEILLANCE CAMERA COMMISSIONER

Annual Report

January 2020 – March 2021

Surveillance Camera Commissioner Annual Report January 2020 – March 2021

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

November 2021

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

Any enquiries regarding this publication should be sent to us at enquiries@obscc.org.uk

ISBN: 978-1-5286-2965-2

E02682343 11/21

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of Her Majesty's Stationery Office

Foreword

Having been appointed to discharge the statutory functions of both the Biometrics Commissioner and those of the Surveillance Camera Commissioner in March 2021, I make this - my first - Annual Report covering a period when the respective functions were, for the most part, the responsibility of my two predecessors. As the functions themselves remain discrete within the legislation[1] I have published two separate annual reports[2].

I am aware that combining the functions was not uncontentious but the rationale for doing so has found corroboration on many occasions, not least of which was the appearance of the previous Biometrics Commissioner before the Commons Science & Technology Committee in June[3] where he spent some time assisting members with issues arising principally from the use of surveillance cameras.

The specific aspects of my role reported on here require me to:
(a) encourage compliance with the Surveillance Camera Code[4]
(b) review the operation of the Code, and
(c) provide advice about the Code (including changes to it or breaches of it)[5].

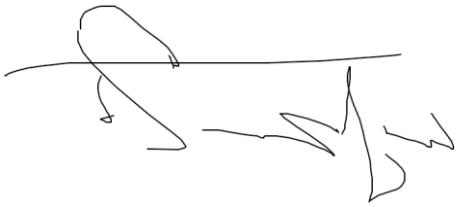
At the time of writing the government is undertaking two statutory consultations that are relevant to my functions, the first of which relates to a revision of the Code of Practice and the other representing a much more ambitious reform of UK-wide data management legislation. My formal submissions to both consultations can be found on my website[6].

Given the extent of change that has taken place in the surveillance camera sector, both in terms of technological capability and public awareness, I would hope that the combined effect of this consultation produces better regulation which meets the legitimate expectations of the surveillance sector, the relevant authorities and, most importantly, the citizen.

In both statutory reports I have highlighted several issues which I believe are relevant to the future of biometrics and surveillance and will return to them in more detail in future annual reports. I also undertake to purge future reports of any but the most

[1] See the Protection of Freedoms Act 2012, Chapters 1 & 2
[2] The report of the Commissioner for the Retention and Use of Biometrics will be available when published at www.gov.uk/government/news/submission-of-the-biometrics-commissioners-annual-report-for-2020
[3] Wednesday 30 June 2021, oral evidence of the former Biometrics Commissioner, Prof Paul Wiles https://committees.parliament.uk/event/5036/formal-meeting-oral-evidence-session
[4] Required to be prepared, issued, and published by the Home Secretary under Ss.29(1), 30(2) and 32(1) of the Protection of Freedoms Act 2012
[5] *Loc cit s.34(2)*
[6] www.gov.uk/government/news/professor-fraser-sampsons-response-to-the-dcms-consultation-data-a-new-direction; Professor Fraser Sampson's response to the Surveillance Camera Code of Practice, 8 September 2021 - GOV.UK (www.gov.uk)

essential acronyms which can become a distraction from the key information particularly to members of the public.



Fraser Sampson
Biometrics and Surveillance Camera Commissioner

Contents

Introduction

Having been appointed by the Home Secretary to cover the functions of both the Commissioner for Retention and Use of Biometrics[7] and the Surveillance Camera Commissioner[8] on 1 March 2021, I am required 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[9]. Thereafter, I am required to publish the report. The period covered by this report therefore covers the exercise of the relevant statutory functions by my predecessor for all relevant months of the past year save one.

In this period there have been many examples of police surveillance systems that have been roundly discredited in various jurisdictions and it is probably true that their use has eroded public trust, perhaps because they were not appropriately validated in advance, perhaps because the police jumped the gun and almost certainly because their use was not properly explained, consulted upon and deployed under clearly defined policies. Whereas facial recognition technology continues to occupy many of the headlines, there are other technologies, biometric or otherwise, which are either waiting in the wings, or are here already.

During this period there has also been a significant judgment from the Court of Appeal[10] in relation to some of the issues arising in the police deployment of live facial recognition technology. While access to effective legal remedy is itself a fundamental human right[11], the recourse to litigation is not necessarily the most efficient or effective way of asserting democratic accountability; it is certainly an expensive and unpredictable way of developing policy[12] and does little to engender public trust. My predecessor, Tony Porter, intervened in the South Wales Police case and had been active in seeking a revision of the Surveillance Camera Code of Practice; he had also proposed a number of amendments to the statutory regime itself[13].

The government's consultation on the Code in response to the judgment has inevitably impacted upon the timing of my report. Moreover, the implications of both consultations referred to in the Foreword are very significant to the functions reported on here and I have therefore included some comment on them.

Since taking up appointment, I and my office have been in continuing dialogue with the Home Office about the proposed revision of the Surveillance Camera Code of Practice. I suggested some changes to the Code, however it was made clear to me that any future revision would exclude any form of structural alteration, any amendment of the Code's principles and further would not extend to a review of the list of relevant authorities bound by its provisions. It is no surprise then that the proposed changes within the draft that was circulated for consultation were modest

[7] s.20(1) of the Protection of Freedoms Act 2012
[8] *Loc cit* s. s34(1)
[9] *Loc sit* s. 35(1)(a)
[10] *R (on the application of Bridges) v Chief Constable of South Wales Police and Ors* [2020] EWCA Civ 1058
[11] Art 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms
[12] See e.g. Rubin and Feeley Judicial Policy Making and Litigation Against the Government, 5 U.Pa.J.CONST.L.617 (2003)
[13] https://www.gov.uk/government/publications/review-of-the-surveillance-camera-code-of-practice

and received as such[14]. In terms of my formal suggestions as a statutory consultee, these were largely dismissed as being 'out of scope'. That my best endeavours to get even a sentence reminding relevant authorities of the ethical considerations were rejected on the grounds that it would be too burdensome is perhaps an indication of just how restrictive this scope – wherever it is to be found – must have been.

Coming within two days of a much wider consultation proposing the 'absorption' of the Surveillance Camera Commissioner's statutory functions under the Information Commissioner[15], the narrow focus of the consultation on the Code has created, perhaps inevitably, a perception that this particular die has already been cast.

On the broader consultation, there are differently held views as to whether the overlaps between the roles and responsibilities of various commissioners for data protection, intrusive covert surveillance and surveillance cameras generally are such that their responsibilities ought to be combined or streamlined in the future. This will ultimately be a matter for others, but I would urge them to consider carefully the beguiling simplicity of generalising this area as merely involving matters of data protection. The abhorrent facts of a case involving the recording of images in a hospital mortuary[16] illustrate very starkly how intrusions into the most private aspects of our lives cannot always be reduced to matter of 'data rights' of a living person.

In the end, people need to be able to have trust and confidence in the *whole ecosystem of surveillance*, which is why singling out one technological application such as live facial recognition is unhelpful and titrating the functions of commissioners is unimaginative. It is clear that the areas of surveillance covered by the Code are heavily and iteratively regulated; there are other areas such as commercial and individual private use of new surveillance technology that fall outside any of the regulatory frameworks[17]. This is a fast-evolving area and the evidence is elusive, but it would be somewhat ironic if the areas left to self-determination were found to present the greatest risk to communities or simply to give rise to the greatest concern among citizens. It may be that some technological surveillance capabilities are so ethically fraught or raise such a level of discomfort from a societal perspective[18], that they can only be acceptably carried out under express authority in advance. That is also a matter of policy for others. But, as we are herded towards a future in which public safety increasingly relies on data being pooled from "disparate databases such as social media, driving licences, police databases, and dark data[19]", a future in which "deep learning enables the system to become more knowledgeable and, as a result, more accurate[20]" we need *as a minimum,* a single set of clear principles by which

---

[14] https://www.bbc.co.uk/news/technology-58206586
[15] www.gov.uk/government/news/dcms-data-reform-consultation
[16] www.bbc.co.uk/news/uk-england-kent-59176555?at_medium=RSS&at_campaign=KARANGA
[17] See examples in: "Facial Recognition Technology: a guide for the dazed & confused", CDEI, https://cdei.blog.gov.uk/2020/06/01/facial-recognition-technology-a-guide-for-the-dazed-and-confused/ https://www.csis.org/analysis/questions-about-facial-recognition; Schneier 2020, "We're Banning Facial Recognition; We're Missing the Point" https://courses.cs.duke.edu//spring20/compsci342/netid/news/nytimes-schneier-facial.pdf; "The Dangers of Unregulated Biometrics", https://www.hrlc.org.au/submissions/2018/5/30/the-dangers-of-unregulated-biometrics-use accessed 2 September 2021
[18] See for example https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3; and https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf pp. 19-28, accessed 2 September 2021
[19] Accenture's Tier 3 in [19]"Seeing What Matters"- A New Paradigm for Public Safety Powered by Responsible AI https://www.accenture.com/acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf accessed 25 August 2021
[20] *Ibid*

those operating surveillance camera systems will be held to account, transparently and auditably. The acid test for the effectiveness of any framework will be how far it allows us to know that surveillance camera systems (what is possible) are only being used for legitimate, authorised purposes (what is permissible) and in a way that the affected community is prepared to support (what is acceptable).

The National Surveillance Camera Strategy

The National Surveillance Camera Strategy (NSCS) was implemented by my predecessor in 2017. There were initially 10 work strands within the strategy, expanding to 11 in 2019. Objectives and delivery plans for each strand were developed for the first 3-year period (2017-2020) and aimed to provide a holistic approach to raising standards across the surveillance industry and encouraging compliance with legal obligations in line with the 12 guiding principles of the Surveillance Camera Code of Practice.

In a document introducing the strategy, the then Commissioner Tony Porter said that he had been impressed with the support, encouragement and engagement across the range of stakeholders for a national strategy. I wholeheartedly share this view and it is clear to me that, without the application, dedication and motivation shown by the various individual experts leads, the regulation of surveillance camera systems in England and Wales would be very much the poorer.

The end result of the National Strategy was identified as "a more transparent, efficient and effective approach to public space surveillance with deliverable outcomes to help people understand the impact of surveillance cameras" with the "true beneficiary being the public"[21].

In early 2020, the NSCS was refreshed and new 'stretch objectives' were implemented by my predecessor, in agreement with each of the strand leads, as part of the process to review the vision, mission and scope of the strategy. These objectives remain relevant for the period 2020-2023 but I will keep them under regular review in light of changing legislation, evolving technologies and increased levels of public awareness and concern.

Each objective has a set of delivery plans set against specific outputs and outcomes. Understandably, some of these timeframes slipped in 2020 as a result of the COVID-19 pandemic and the impact this inevitably had on the various work streams. The hardest hit was arguably the Civil Engagement strand, with objectives to engage with citizens through public debates and hold surveillance camera 'open days' becoming unachievable with the announcement of lockdown restrictions and the inevitable effect this had on the ability to gather in large groups. The Standards and Certification strand also had deliverables put on hold with schemes ready to be set in motion, but with conferences at which the schemes were due to be launched being cancelled, on some occasions more than once.

It is clear the pandemic has impacted, and continues to impact, upon many sectors across the UK, including the surveillance camera industry. Nevertheless, there is still a tremendous amount of work being undertaken by the strand leads, all of whom work on a *pro bono* basis, and their achievements have been recognised by both my predecessor and me. I am very grateful for all that the strand leads have done, particularly in these difficult periods when people have been faced with their own personal and professional challenges and I am looking forward to working with them in the future to continue the momentum they have been so instrumental in creating.

[21] https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales

Chapter 1 – Standards & Certification

The objectives for the Standards and Certification strand are to produce guidance and requirements, based on agreed standards, for manufacturers, consultants, installers and monitoring centres. Those standards are intended to ensure a quality management approach from the initial capture of the surveillance camera image through to the product passing onto the police and all points in between. In addition to meeting the relevant quality, the requirements and associated guidance must also be practical, affordable and reasonable, making this a particularly challenging task.

Two new certification schemes are due to be launched in 2022 for service providers and monitoring centres (see below). A further area where requirements and guidance are needed is for consultants advising on the design of surveillance camera systems. The aim for the next reporting period is to produce requirements and guidance for those consultants. These might have mandatory requirements as well as desirable requirements and could be either self-assessed or third party assessed (or both). In establishing these standards, it will be important to obtain the views of the new Forensic Science Regulator, particularly as the product of surveillance camera systems currently covered by the Code is principally used to investigate crime or support a prosecution.

1.1 Standardising video surveillance outputs

In 2020 a video surveillance systems standard output working group was established by Alex Carmichael, Executive Chair of the Security Systems and Alarms Inspection Board (SSAIB), and leading expert on Standards and Certification.

In his blog 'Standardising video surveillance outputs'[22] in June 2020 Alex said:

> "Most manufacturers have bespoke systems with proprietary software and the current speed of technology change means that manufacturers are looking to be first to market with new innovative products. This is understandable, but one of the vital aspects of any surveillance camera system should be its ability to provide the right surveillance data in the right format, at the right time and to be easily transferred to law enforcement agencies. This is not always the case in surveillance systems.
>
> "…the working group is looking at condensing the issues the police and courts have with video data from surveillance camera systems and put them into a document which, will set out the current situation and problems, possible solutions and recommendations.
>
> "The video surveillance systems standard output working group is made up of National Police Chiefs' Council and individual police forces, the Courts and Tribunal Service, police forensic experts, the Centre for the Protection of the National Infrastructure, the National Association of Surveillance Camera Managers and others. The group has a wealth of

[22] https://videosurveillance.blog.gov.uk/2020/06/24/standardising-video-surveillance-outputs/

experience in video output data issues, but understands it is only by talking and working together with manufacturers will real change happen and this can only be of benefit all those involved in, and those who use surveillance camera systems.

The group has been working on producing documents that standardise video surveillance output. There have been significant challenges to overcome around the education of system users, commonalities of the technology being manufactured and deployed, and more generally, the multitude of processes involved in the retrieval of data in a variety of different scenarios. Those documents are nearing completion and will be published on my website in the next reporting period.

1.2 Third-Party certification

The third-party certification scheme continues to grow and by March 2021, there were approximately 100 organisations that had achieved certification against their use of various surveillance camera systems (an increase of over 50% in the last 3 years). This includes Closed-Circuit Television (CCTV), Body-Worn Video (BWV), Automatic Number Plate Recognition (ANPR) and drones. We have yet to see any organisations apply for certification against their use of facial recognition technology but with its ever-increasing use, both in the private and public sector, it seems inevitable that this will happen before too long.

My office continues to encourage all organisations, whether they are a 'relevant authority' or otherwise, to apply to the certification scheme, which gives them the opportunity to demonstrate visibly their compliance with the Surveillance Camera Code of Practice and display the certification mark on their website and any other publicity materials. Certification should go a long way to assure people that where surveillance camera systems are being operated, it is being done in a way that is proportionate, transparent, effective, and only where necessary to meet a pressing need. Certification against the Code's principles by commercial camera operators also shows a commitment to standards and transparency that is becoming increasingly relevant in the otherwise unregulated area of 'private' surveillance.

There is still work to be done however. Although the number of local authorities achieving certification is continuing to expand, this is still a relatively low number in proportion to the total number of local authorities that are using surveillance camera systems. I would also like to see the number of police forces achieving certification increase and would hope that their recently-elected local policing bodies[23] are able to reflect the views of their communities in holding their chief constables to account for the use of surveillance camera systems.

Given the multitude of private sector organisations that are engaged with the scheme, including high street retailers, universities and the parking sector, there is a risk that the public bodies under a legal obligation to have regard to the Code are being upstaged by other organisations that are seeking certification entirely of their own volition. Insofar as central government is concerned, for departments not to adopt the Code is very difficult to explain still less defend. My office has worked tirelessly to

[23] Police and Crime Commissioners and Mayor's offices for policing and crime as provided for under the Police Reform and Social Responsibility Act 2011, s. 7(1)

promote the scheme to a whole range of different surveillance camera operators but indications are that for some organisations the process of achieving certification can be a complicated one. We will continue to work with all organisations aspiring to the Code's standards – including central government – to offer them support and guidance, and there are plans to embark on a number of presentations throughout the upcoming year.

1.3 Secure by Default

Secure by default is a self-certification scheme which allows manufacturers of surveillance camera devices and components to demonstrate clearly that their products meet minimum requirements relating to cyber-security, to ensure that they are secure by default and secure by design.

The scheme was designed for manufacturers by manufacturers and provides assurance for end-users (installers and operators) that the devices they are using meet a minimum level of cyber security, such as requiring default password settings to be changed on installation.

Manufacturers apply for the mark by submitting a simple form to my office who then assess the detail and, if the application meets the criteria, issue the mark and certificate. The scheme is administered with significant support from the National Surveillance Camera Strategy cyber expert, Mike Gillespie the Director of Advent IM and Buzz Coates from Norbain.

Several manufacturers have been given the mark throughout this reporting period for a multitude of surveillance camera devices. A list of manufacturers who have the mark is available on my website.[24]

The invaluable work under this strand is of particular importance in light of recent concerns about risks from cyber-attack. While advice is readily available from the National Cyber Security Centre and the Centre for the Protection of National Infrastructure, the proliferation of surveillance camera systems and advances in the attendant technologies possibly represent a new manifestation of an enduring risk. The increasing interoperability/interdependency of systems intended to keep our citizens safe raises further considerations about the provenance and practices of manufacturers and service providers. As the features of biometrics and surveillance systems become more sophisticated and further embedded in the infrastructure of our everyday lives, they will demand renewed attention from us all.

1.4 Certification for service providers

This scheme was designed as a deliverable of the Standards and Certification strand of the NSCS and is aimed at organisations who install, integrate and design surveillance camera systems – which have been termed 'service providers'.

The scheme sits alongside my other certification schemes and will raise standards in relation to how surveillance camera systems are designed, installed and maintained.

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

This will mean that organisations operating surveillance cameras will have systems that fully meet their needs, the police will have access to better video evidence and the public can have a greater level of reassurance over the integrity of those systems. It is anticipated that organisations will be specifying which service providers have this certification mark in tendering processes. The scheme will be fully administered by the third-party certification bodies.

This scheme was due to be launched in May 2020 at the IFSEC conference in London but owing to the COVID-19 pandemic, it has been postponed until 2022.

1.5 Certification for monitoring centres

This scheme was also designed as a deliverable of the Standards and Certification strand of the NSCS. It is aimed at monitoring centres.

There are two different types of Surveillance Camera Monitoring Centre, one where a surveillance camera system owner contracts out the monitoring (Contracted) and the other where a surveillance camera system owner monitors their own system. There is also a Contract Monitoring Service which can provide personnel to the two types of monitoring centre.

The new scheme has been developed to support both and to ensure that monitoring centres operate to relevant recognised British and international standards. The scheme will be fully administered by the third-party certification bodies. Once again, we will be liaising closely with the new Forensic Science Regulator in setting and maintaining standards for monitoring centres.

This scheme was due to be launched in June 2020 at the National Association of Surveillance Camera Managers (NASCAM) but owing to the COVID-19 pandemic, it too has been postponed.

Chapter 2 – Civil Engagement

The Civil Engagement strand of the National Strategy has evolved over a 5-year period. Initially, activity focussed on identifying objectives, deliverables and measures, and then subsequently on enacting them. This strand is unique, as it provides a key link between me as the Commissioner, and public and expert opinion. This engagement is critical in ensuring that I have a sense of public attitudes towards surveillance cameras and mechanisms for engaging with civil society, something that has become increasingly relevant in some developments such as live facial recognition technology.

In practice, the strand activities have served three main purposes:

1) delivering elements of the National Strategy (the intended purpose);

2) drawing attention to the functions of the Surveillance Camera Commissioner; and

3) providing access to key organisations and individuals having specific interests in the area of public space surveillance.

The previous Commissioner often suggested that Professor William Webster (Director at the Centre for Research into Information Surveillance and Privacy (CRISP) and the expert leading this strand), speak with public agencies about how to organise their public engagement and what should be conceived as good or best practice. I am keen to support this initiative. This strand has been delivered with limited resources, with utilised networks embedded in the CRISP research centre and Home Office resources for publicity materials.

Since the objectives of the strand were agreed, a number of engagement mechanisms and activities have taken place. These include a stakeholder workshop, a survey of local authorities, public facing panel sessions (such as the Question Time Event in 2018), public lectures (CRISP Annual lecture and IFSEC), publications in the popular press (broadsheets and The Conversation for example) as well as a range of activities associated with the first Surveillance Camera Day in 2019. The Surveillance Camera Day was a culmination of these activities and was deemed to be a great success, and there is clear evidence that it drew attention to a national ‘conversation’ about surveillance cameras. The event incorporated media activity (TV and radio), including dedicated social media activity, information sheets for providers, posters, and a ‘doors open’ initiative.

The plan for 2020 had been to build on what had already been achieved and to take advantage of the materials and practices established for the initial event. The materials developed for this were designed to be reused from one year to another. Initially, the Surveillance Camera Day was scheduled to take place in June 2020 alongside the IFSEC conference. However, the onset of the Covid-19 pandemic meant this conference was initially postponed until the autumn and then cancelled. The team kept an open mind about whether to run the event ‘virtually’ or whether to wait until the IFSEC conference ran. Ultimately, uncertainty around lockdown restrictions and the change in Commissioner meant it was decided to postpone the event until 2022.

A number of new activities were planned for 2020. First, the team had provisionally organised a number of school presentations to take place in the run up to the Surveillance Camera Day. These were to be delivered by trusted academic colleagues across the UK. Second, in spring 2020, several events in Parliament were planned around the topic of surveillance cameras, oversight, governance and/or Automated Facial Recognition (AFR). Planning for these was at quite an advanced stage but the Parliamentary timetable was congested with issues relating to the United Kingdom leaving the European Union and then the Covid-19 pandemic. These activities can readily be revisited and integrated into a broader engagement plan.

The Civil Engagement strand objectives remain very relevant and the need to secure ongoing engagement and awareness building with civil society and the general public increases with every technological development and related news story. Surveillance technology evolves quickly and policy initiatives having surveillance implications (such as COVID-19 'passports') need to be consulted upon and drawn to the attention of the public, along with revision of the Code itself. This is a key part of ensuring that public space surveillance as covered by the current framework is understood.

Chapter 3 – Policing

Police forces and their elected local bodies in England and Wales are 'relevant authorities'[25] and, as such, must have regard to the 12 guiding principles in the Surveillance Camera Code of Practice when operating any overt surveillance camera system in public spaces. My office has conducted biennial surveys in 2017 and 2019 to understand the levels of police compliance with the legislation and the Code.

My predecessor made a number of recommendations to police forces, including the appointment of a Senior Responsible Officer responsible for ensuring compliance with the legislation and the Code.

In 2020 my office compiled a comparison report of the survey results, to understand where forces have raised standards during the 2-year period between surveys, and where improvements need to be made.

It is worth noting that there were some differences in the way data was collected in each survey, which in some areas has impacted on the effectiveness of comparison[26].

This exercise has produced some interesting results. For example, the percentage of forces using CCTV, UAVs (drones) and body worn video has increased (ANPR use is the same). Levels of compliance have also increased – but in all cases where we hold data, the percentage of forces using a Self-Assessment Tool (SAT) to demonstrate compliance has decreased or not changed. I would like to work with police forces to drive up completion rates and this is a key area of the national strategy. Although there is no legal obligation to complete a SAT, it would assist forces in identifying areas for improvement and consequently increase their compliance levels further.

I would also like to concentrate on providing more guidance on partnership arrangements and the types of surveillance camera systems that fall into the 'other' category as it was these two areas that seemed to cause some confusion and an inconsistency in how forces responded to questions.

I have plans to continue the biennial surveys and my office will be contacting police forces in 2022.

3.1 Regional Senior Responsible Officer (SRO) Meetings

During my predecessor's tenure, Superintendent Simon Inglis of West Midlands Police established a regional overt surveillance group to bring together senior responsible officers with responsibility for ensuring compliance with s. 33(1) of the Protection of Freedoms Act (PoFA) 2012 and the SC Code, in respect of all overt surveillance camera systems that their forces operate.

My visits to police forces over the past 6 months have found consistent evidence of Supt Inglis's leadership and the impact that this has had on helping forces improve their understanding of, and compliance with, the Code. With the significant support of his regional colleagues, this group has made considerable progress and is a great

[25] as defined by section 33(5) of the Protection of Freedoms Act 2012

[26] for example, in 2017 data was collected on internal CCTV systems and CCTV systems as a whole, whereas in 2019 data was collected separately on both internal and external CCTV systems.

example of how police partnerships can work effectively in advancing compliance with the legislation and the Code.

As Supt Inglis puts it:

"The regional meeting structure has been invaluable. It has provided a mechanism for good practice to be identified, shared and implemented, and it enables a greater understanding of all covert surveillance matters e.g. one force identifying an area of business which may have otherwise been inadvertently overlooked by another.

"Additionally, the approach has introduced an element of moderation and consistency. On a personal note I have drawn on the regional meeting effectively to support force level delivery. It has put overt surveillance on our radar and acts as a barometer as to where we are at with compliance and listening to force updates helps to understand where our potential gaps are and how to fill them. The discussions around national activity also assists with horizon scanning and has certainly helped to drive business across our force area"

I fully support this ongoing work and am working to encourage other regions in England and Wales to use this group as a model to establish similar ways of working.

3.2 Facial Recognition Technology

Facial recognition technology has been the focus of much surveillance-related news and internal debate over the reporting period, with the legal challenge brought against South Wales Police for their use of the technology attracting significant public and professional attention[27].

My predecessor was an intervener in the case and provided a submission to the Court of Appeal with support from Professor Pete Fussey, the NSCS leading expert on Human Rights, Data and Technology. This submission set out his legal argument and socio-legal research-led insights into the uses of AFR, emphasising the human rights implications generated through operational uses. Professor Pete Fussey of Essex University is an internationally recognised expert on the uses and impact of surveillance and advanced digital technology for law enforcement, national security and public protection. Professor Fussey was invited to conduct a review of the Metropolitan Police Service's trial of new technology in this respect and it is a matter of some regret that his report[28] was later criticised when its published findings were received[29]. The contribution of experts such as Professor Fussey to the credibility of the national surveillance strategy and the professionalisation of surveillance use by the police cannot be overstated and I am personally very grateful for his continuing support.

While the South Wales Police litigation predates my appointment, it is clear to me that several of the facts in issue arose from wider data protection and equality obligations arising in the context a surveillance technology. Following a first instance decision in the High Court, in August 2020 the Court of Appeal concluded that there were "fundamental deficiencies" in the legal framework surrounding the police use of live

[27] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058
[28] https://www.hrbdt.ac.uk/hrbdt-researchers-launch-new-report-on-london-metropolitan-polices-trial-of-live-facial-recognition-technology/
[29] See e.g. techthelead.com/the-london-polices-facial-recognition-system-is-wrong-81-of-the-time/

facial recognition (LFR). Clarifying a number of central issues in relation to the legal framework governing surveillance cameras, the Court found that the appellant's rights had been breached, in particular noting that the South Wales Police Data Protection Impact Assessment (DPIA) did not comply with the Data Protection Act (DPA) 2018 and that the police had failed to discharge their obligations under the Public Sector Equality Duty arising from the Equality Act 2010.

Of particular relevance to this report are the Court's observations regarding the Surveillance Camera Code. The judgment says: [30]

> "…it seems to us that [the Code] could in principle also deal specifically with what the requirements are for inclusion on a police force's watchlist. It could also deal with what policies should contain in relation to the location of the deployment of AFR Locate. As we have said earlier, the question whether such policies must be set out in a national document such as this Code or whether they should be set out in local policies determined by each police force is not a matter for this Court. It may be prudent, however, for there to be at least consistency in the content of local policies and that might be the appropriate subject of an amendment to the Code by the Secretary of State."

Mr Porter responded to the judgment and published a statement[31] which included the following:

> "I note the issues in the judgment regarding bias that can be inherent in facial recognition algorithms. Use of this technology will not and should not get out of the gate if the police cannot demonstrate its use is fair and non-discriminatory. I will consider how I can amend my guidance to ensure police forces are aware for the potential bias in systems and also consider what more can be done with manufacturers of the technology to eliminate it.
>
> I very much welcome the findings of the court in these circumstances. I do not believe the judgment is fatal to the use of this technology, indeed, I believe adoption of new and advancing technologies is an important element of keeping citizens safe. It does however set clear parameters as to use, regulation and legal oversight."

The Home Office has included a section in the proposed revision to the Code which, at the time of writing, has been published for consultation.

3.3 Facing the camera

Following the judgment, my predecessor consulted with the police, the Association of Police and Crime Commissioners (APCC), academia, legal advisers, the NSCS leads and other stakeholders, to revise his guidance *"The Police Use of Automated Facial Recognition Technology used with Surveillance Camera Systems*" which was published in March 2019.

[30] at para 118
[31] https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition

In December 2020 he issued 'Facing the Camera[32]', a new guidance for police forces to follow when considering the deployment of LFR surveillance camera technology in public spaces. This guidance makes several recommendations to both the police and the public, for example:

- the importance of the public sector equality duty.
- due diligence in procurement and deployment of technology.
- integrated risk and threat impact assessments.
- meaningful public engagement prior to deployment.
- the important role of police and crime commissioners' governance when holding chief officers to account.
- the potential role for ethics committees to provide independent scrutiny of operational intent, decisions, and actions.
- the structures, credentials and potential for risk associated with the role of human decision makers.
- strategic oversight and independent decision making which approves police conduct.
- overt and covert considerations and the use of third-party systems.

3.4 Police engagement in National Surveillance Camera Strategy

Assistant Chief Constable (ACC) Jenny Gilmer, National Police Chiefs' Council (NPCC) lead for CCTV, leads the policing strand of the NSCS. She has supported the biennial surveys that my office has conducted in order to understand the level of compliance with PoFA and the SC Code across police forces in England and Wales. Throughout 2020, ACC Gilmer tasked the national CCTV working group to review all existing material that relates to the management and processing of CCTV, ensuring that the whole end-to-end lifecycle of CCTV was covered. This led to a review of the existing College of Policing material and any other training and procedural guidance that is being used across law enforcement. The aim was to provide updated process and training material to support a more effective and efficient way of managing CCTV across law enforcement.

One deliverable of the NSCS is to establish data collection processes which enable all forces to develop an evidence base which in turn can inform best practice, share it with partners, and indicate positive outcomes from the use of video surveillance camera systems.

In a recent blog, Andy Read the NPCC Capabilities Manager for CCTV said:

> "To the Police, CCTV evidence is the primary consideration in around 90% of all investigations and is the main detection factor in over one third of all justice outcomes. CCTV is also 100% effective for establishing crimes have been committed, linking crimes, identifying victims, establishing cause of death, eliminating post charge suspects, charging suspects, and providing admission of guilt, and is over 96% effective in identifying persons of interest.

[32]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

> In times of austerity it is even more critical for the police to work with local authorities to demonstrate this effectiveness and prove the legitimacy and justification of CCTV evidence."

The contribution of CCTV to the investigative and criminal justice process means it will be important to maintain a close working relationship with the new Forensic Science Regulator.

Research and data collection are ongoing across a number of areas and the proposal for use of surveillance camera evidence to be added to the Annual Data Requirement is currently under review, which will support the analysis of crime and policing related statistics.

3.5 Automatic Number Plate Recognition

Automatic Number Plate Recognition (ANPR) continues to attract an enormous amount of public attention, focussed in both the public and private sector. Police use of this technology has resulted in the culmination of the largest non-military database in the UK, with approximately 11,000 cameras capturing and submitting around 50 million reads to national police ANPR systems every day[33].

There is reasonable conjecture that these figures decreased during 2020 when lockdown restrictions will have had an impact on how often, and how far, people were able to travel. However, as lockdown measures have eased and we have seen a return to a more conventional pattern of road use, the amount of ANPR data being collected and retained has inevitably returned to those same levels that were being recorded prior to the pandemic.

Reports in the media highlighted concern at how ANPR (and drone technology) was used by the police to enforce the law regarding essential travel throughout the pandemic. This reflected some legitimate concerns around the expansion of ANPR use and the correlative intrusion into citizens' expectations of privacy. My office has been working closely with the police to encourage compliance with the Surveillance Camera Code and to ensure that where these systems are being deployed, their use is proportionate, necessary, transparent and in pursuit of a legitimate aim.

Since 2018 my predecessor chaired an ANPR Independent Advisory Group (IAG) at the request of Chief Constable Charlie Hall, the NPCC lead on ANPR. The group consists of police, Home Office officials, other regulators, academics and industry experts, all of whom provide advice and challenge on the legitimate, transparent, proportionate and ethical use of ANPR by police, law enforcement agencies and other non-statutory ANPR users.

The IAG was unable to meet face-to-face throughout 2020 because of pandemic restrictions but was able to have a tele-conference early in the year. Despite the many challenges arising during the pandemic, the group have continued to offer their support and guidance on myriad issues, and both Tony Porter and Charlie Hall have been very

[33] https://www.police.uk/advice/advice-and-information/rs/road-safety/automatic-number-plate-recognition-anpr/

diligent in bringing me up to date on the positive impact the group has had in shaping the development and evolution of the National ANPR System.

The standards for the use of ANPR in policing and law enforcement are comprehensive and stand out as providing a robust and exemplary framework fundamental to assuring the transparent and proportionate use of ANPR technology. Members of the IAG have provided valuable guidance in the development of national training products for the new National ANPR Service, ensuring awareness of data protection and data management responsibilities are embedded alongside skills training, and tested prior to system access.

Members also provided valuable support to the ANPR Value Model which was developed as part of the National ANPR Portfolio to provide a baseline for the ANPR maturity of police forces and assist with optimising the benefits that can be derived from ANPR.

I am delighted that Charlie Hall has asked me to chair the IAG during my tenure and I am looking forward to taking over the responsibilities and duties associated with this role.

3.6 Green Number Plates

In January 2020, my predecessor responded to the Department for Transport consultation on the introduction of Green Number Plates for Ultra-low Emission Vehicles[34] having collated comments and guidance from members of the ANPR IAG. The key points in his response are as follows:

- The government's policy to reduce emissions and encouraging road users to switch to cleaner vehicles is supported. However, it is important that the design of green number plates does not impact on the National ANPR Service (NAS).
- IAG members have expressed concerns that this extension of ANPR functions is not justified and there is limited evidence that it would benefit society. Therefore, its legality is questionable.
- Extending the use of the role of ANPR is beyond its initial purpose and causes further concern over its legitimacy. There are ongoing issues around the lack of statutory footing for ANPR. There are also concerns around proportionality and who can access the data.
- If local authorities intend to use ANPR to support clean air zones, they must have regard to the SC Code. It is recommended they complete a SAT to assess compliance and to help identify any non-compliance issues. This should be reviewed at least annually.
- Consideration should be given to any incentives of having a green number plate and the effect this might have on individuals mispresenting or cloning number plates. This subsequently leads to inaccurate data going into the National ANPR system and impacts on operational policing. The process for obtaining green number plates needs to be tightly controlled.

[34]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861114/Green_Number_Plate_Consultation_Response.pdf

3.7 Cloned and defective number plate sub-group

A sub-group of IAG members was formed in 2019 to hold informed discussions around the manufacture and supply of non-compliant and cloned plates and the impact this has on operational policing and the accuracy of data going into the National ANPR System. The sub-group was chaired by the Driver and Vehicle Licensing Agency (DVLA) and members included representatives from the Home Office, my office, the British Number Plate Manufacturers Association, the NPCC and the APCC.

In July 2020 the sub-group produced a report, commissioned by my predecessor, with recommendations and policy proposals to address issues in the manufacture and supply chain and limit the number of non-compliant and cloned number plates entering the market. The nine recommendations were divided into three main areas (Prevent, Identify and Enforce) and can be summarised as follows:

1. The inclusion of greater security features within the plate.
2. Limiting the availability of component materials and introducing a tracking system to identify the origin of manufactured or assembled plates.
3. Formal licensing of manufacturers with third party certification of component materials.
4. The introduction of an increased, annual fee.
5. Formal licensing of suppliers with new eligibility application criteria.
6. Digital solutions to enable licensed suppliers to authenticate and authorise individual rights to a number plate.
7. The development of a structured and tailored communication package for suppliers and customers.
8. Increased penalties and simpler prosecution routes. The application of existing systems to identify non-compliance.
9. Greater collaboration with partners to align policies.

My predecessor wrote jointly with the NPCC and APCC leads to the Minister for Crime and Policing, Kit Malthouse and the Parliamentary Under Secretary of State Baroness Vere, requesting that this work be added to the agenda at the upcoming vehicle crime summit between the Home Office and Department for Transport with a view to progressing the recommendations in the report. Ministers endorsed those recommendations, although it was later decided that the vehicle summit was not the right mechanism for pursuing these matters.

Discussions are currently ongoing with ministers, DVLA, the police and other interested parties to devise a strategy for implementing the recommendations where that is feasible. The biggest challenge it seems is collating an evidence base to demonstrate that a change in legislation is indeed necessary. I expect the issue of cloned and defective plates to be an ongoing topic for discussion.

Chapter 4 – Local Authorities

In February 2020 my predecessor wrote to the Senior Responsible Officer for every local authority in England and Wales, responsible for ensuring compliance with the Protection of Freedoms Act 2012 (the Act). They were asked to complete a survey to account for the surveillance camera systems that their local authority operated in public places and which fell within the remit of the Act, and the extent to which the operation of those systems complied with that legislation[35].

It should be noted that the survey was conducted at the start of the COVID-19 pandemic, which caused many local authorities to divert resources to provide frontline services to the communities they serve as well as dealing with staff absences. Additionally, this was the first survey of its type conducted and required significant information gathering by authorities and working across organisational boundaries to provide a full response. Despite these challenges the response rates were relatively good with 184 authorities responding, representing approximately a 50% response rate. The information provided by those local authorities has not been independently audited, inspected or verified.

I praise the efforts of those involved in collating the relevant information to respond to the survey, with thanks also to the Public CCTV Managers Association and the National Association of Surveillance Camera Mangers/CCTV User Group who helped with the construction of the survey questions.

It was reported that, with the exception of one local authority, there were appointed Senior Responsible Officers with specific responsibility for ensuring compliance with the Act and the Surveillance Camera Code of Practice. Only one local authority claimed not to be using any surveillance camera systems, and there were no reports of any local authority using facial recognition technology.

In recent years we have seen austerity measures affect the operation of CCTV, with more and more cameras being taken out of operation owing to funding pressures. The overwhelming majority of local authorities reported funding the operation of their own main/town centre systems.

It was reported that over 80,000 cameras were in operation across 6,000 systems, the majority of these being CCTV cameras, although more recent innovations such as dash cams and body worn video were also in use. The largest number of systems were operating in and on vehicles (1,240), followed by municipal buildings (931), housing (796) and town centres (370). Housing accounts for the largest number of cameras (16,901), followed by town centres (14,702), municipal buildings (12,051) and vehicles (8,842).

Local authorities reported that for the majority of main town centre schemes, a SAT[36] had been completed. This tool was first published by my predecessor in 2014 and is designed to help organisations identify if they are complying with the principles of the

[35] "Public place" has the meaning given by the Public Order Act 1986 s.16(b) and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission

[36] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

Surveillance Camera Code of Practice. There is no legal requirement to complete a SAT, but for the purposes of this survey, it was this that was used to gauge compliance levels. Where a SAT had not been completed, my office did not ask local authorities if compliance was being demonstrated by other means. Outside the main town centre system, SAT completion rates range between 26% and 58%. There is clearly more work to be done in this area and my office continue to work closely with organisations such as the CCTV User Group/National Association of Surveillance Camera Managers and the Public CCTV Managers Association to help promote the SAT to drive up completion rates.

Questions were also asked around the third-party certification scheme, which has been operating since 2015, enabling organisations to clearly demonstrate their compliance with the Surveillance Camera Code of Practice through having their systems audited by an independent UKAS accredited certification body. Over 100 organisations at present can display my certification mark, including 60 Local Authorities. It is seen as the 'gold standard' with regard to the operation of surveillance camera systems.

The survey asked local authorities if they had not obtained third-party certification and why they had chosen not to do so – 162 authorities answered this question. Nearly 50% cited the need to improve or review systems and procedures before certification could be obtained. Almost a quarter of respondents said they did not know that certification exists, which is concerning given the length of time it has been running and the promotional work my office had conducted over the last few years. Some local authorities said they felt certification was not necessary which, while not surprising given there is no legal obligation to attain it and not does not in itself reflect compliance, is disappointing. Not having the knowledge to apply for certification was cited by 10% of respondents, and cost was also reported as a precluding factor when making decisions about certification.

The survey also asked if local authorities were working in partnership with other organisations – 157 authorities answered this question. The Surveillance Camera Code makes it clear that whenever a local authority engages in a partnership with a third-party operator of a surveillance camera system then the authority remains bound by its provisions. Those responsibilities do not apply to the third party unless they are themselves a 'relevant authority'[37]. The relevant paragraphs of the SC Code are as follows:

> 'The duty to have regard to this Code also applies when a relevant authority uses a third party to discharge relevant functions covered by this Code and where it enters into partnership arrangements.' (para 1.11).
>
> 'Where a system is jointly owned or jointly operated, the governance and accountability arrangements should be agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and

[37] As defined in s.33(5) of the Act

procedures for the resolution of any differences between the parties or changes of circumstances.' (para 3.4.2).

Most local authorities reported working in partnership with the police, with footage from their CCTV systems being used in criminal investigations, and to assist the police responding to live incidents. Half of the respondents said they work in partnership with other local authorities, and many worked with others such as Business Improvement Districts, Housing Associations, Professional Football Clubs, Hospitals and transport providers. Over a quarter of local authorities have cameras operated on their behalf by a third party. Where partnership arrangements are in place, we would expect this to be supported by robust governance and agreements.

Approximately 60% of respondents are reviewing over 250 pieces of footage each year, with over a quarter carrying out more than 1,000 reviews annually.
The results of the survey show that 40% of authorities give the police 250 or more pieces of media annually and just over 20% are providing over 500 pieces of media every year. It is estimated that there were a combined 184,875 reviews taking place and 63,500 pieces of media given to the police annually. That equates to an average of 1,027 reviews and 359 pieces of media given to the police per authority each year. We did not seek any information on the value of the media being provided, although anecdotal evidence suggests that it is inconsistent.

Taking the findings from the survey as a whole, my predecessor made 3 recommendations designed to help local authorities fully meet the requirements laid out in the Act and the SC Code:

1. It is recommended that all local authorities conduct a review of all surveillance camera systems operated by them to establish whether those systems fall within the remit of section 29(6) PoFA. The advice of authority legal advisors may be required in some circumstances. Where systems are so identified there should be processes in place that enable the local authority to discharge their responsibilities effectively under the PoFA in respect of those systems and ensure they comply with the legislation. This can be achieved by the completion of the SAT which, when completed, will signpost any barriers to meeting the 12 guiding principles in the SC Code.

2. It is recommended that local authorities ensure that effective governance arrangements are in place with regard to <u>all</u> surveillance cameras they operate in public places across the breadth of their organisations. This should include the:

    - appointment of a single point of contact (SPOC) with regard to surveillance camera issues who can support senior responsible officers (SRO) on operational matters such as when new systems are proposed or upgraded;
    - establishment of processes to ensure continued compliance with relevant legislation for systems via completion of SATs and DPIAs.

- establishment of processes to ensure any new or upgraded systems meet legal requirements.

3. Linked to recommendation 2, authorities should consider whether there are sufficiently robust governance and oversight arrangements across the authority, which ensure that partnership arrangements with third-party operators of surveillance camera systems, particularly those systems with additionally intrusive capabilities or otherwise providing a heightened risk of legal or reputational impact, are:

    - readily identifiable by, or notified to, an SRO;
    - conducted in accordance with the law, the SC Code, regulatory guidance and policy;
    - documented in a written protocol (Service Level Agreement, Memorandum of Understanding etc); and
    - there is clear local authority responsibility and accountability established for the use of a third-party system in partnership.

It is clear from the survey results that more support needs to be given to local authorities to drive up compliance levels across the breadth of surveillance camera systems they operate. This continues to be a priority for my office, and I would expect to see an upward trend of compliance when a second survey is carried out in 2022.

4.1 Service level agreements

A deliverable under the policing and local authority strands of the National Strategy has been to design an effective Service Level Agreement (SLA) specifically for partnerships between relevant authorities[38] regarding the operation of surveillance camera systems.

The aim of this objective is to help facilitate effective partnership addressing several areas of collaborative working, including Information Sharing Agreements, directed surveillance, vetting, training, sharing live images, feedback and welfare of staff. It also sets out standards and procedures that will in turn reassure the public that where surveillance camera systems are being operated, their use is proportionate, necessary, and lawful.

Tony Gleason, local authority lead on the NSCS and chair of the Public CCTV Managers' Association, which represents managers from over 200 local authorities, has worked closely with Assistant Chief Constable Jenny Gilmer (the policing lead on the NSCS and NPPC lead on CCTV), the National Association of Surveillance Camera Managers, the London CCTV Managers group and the Local Government Association to progress this deliverable and I am very grateful for his continuing efforts.

The agreed SLA guidance and framework document[39] enables information sharing and feedback between both parties, provides further evidence of the value of surveillance camera systems and drives up best practice and performance delivery outcomes. It is of the utmost importance that we continue to provide local authorities

[38] Per s.33(5) of the Act
[39] https://videosurveillance.blog.gov.uk/2021/08/19/framework-service-level-agreement/

and the police with tools to ensure they are able to use their surveillance systems to the best possible standard. As we move forward, further opportunities for promoting the SLA are being explored.

Chapter 5 - Installers, Manufacturers and Designers

In September 2019 Tim Raynor, a Video Product Manager and AIPMM Certified Product Manager for Johnson Controls, became the strand leader for Installers, Manufacturers and Designers, inheriting the work that had been carried out by his predecessor, which was the creation of a “Buyers’ Toolkit” created to assist end users to make informed choices on the purchase of a video surveillance system.

There was also an “Owner/Installer guidance document” designed to explain responsibilities of each role when using the twelve guiding principles of the Surveillance Camera Code. It was agreed that the documentation should be reviewed and updated in line with changes that were happening in the security market such as the adoption of automatic facial recognition.

In early 2020 feedback for the proposed changes had been collated and a further review was planned to ensure the group were aligned. However, these plans were suspended as a result of unforeseen circumstances relating to the COVID-19 pandemic and are expected to be revitalised and progressed throughout the next reporting period.

Chapter 6 - Training

The training strand of the Strategy is led by Gordon Tyerman, Managing Director, CCTV Training & Logistics. Setting high standards of training is essential if the public are to have faith in how surveillance camera systems are operated in an open, transparent and ethical manner. If standards are to be raised, training needs to be harnessed across the relevant surveillance camera sectors and be visible and available.

The training strand seeks to drive up standards across roles in the industry including designers, installers and managers of surveillance camera systems by providing information and access to relevant training courses.

In a newsletter article published by my predecessor, Gordon said:

"With the development of technology and surveillance camera systems moving at such a fast pace, it is essential we train our designers, installers, managers and operators to the highest level. CCTV images have become the "go to" evidence for police forces across the UK and civil litigation make use of CCTV images in cases every day. My aim is to provide a comprehensive reference document which will give current and future users of CCTV surveillance a place to find how they can develop the skills and knowledge they will need to deliver a gold standard CCTV for the UK. I am also involved with the NPCC[40] on the development and introduction of an updated national standard for the different roles within the police service when dealing with CCTV surveillance evidence."

The strand objective of collating various training solutions is complete to a point, with the database of training provision covering the various roles within the CCTV world and there are limited options for some of those roles in training. Unfortunately, publishing the document has proved problematic owing to the limitations placed on publications via the GOV.UK website[41]. My office is working on finding a solution and looking into the possibility of hosting this document on an alternative platform.

[40] https://www.npcc.police.uk/

[41] Reliance on this government website has also been raised by the previous Biometrics Commissioner and various stakeholders as diluting the independence of my roles and I am looking at alternative options.

Chapter 7 – Legal Regulation

My role as Surveillance Camera Commissioner was created by virtue of section 34 of the Protection of Freedoms Act 2012. My statutory functions under that legislation are to:

a) encourage compliance with the Surveillance Camera Code of Practice
b) review the operation of the Code, and
c) provide advice about the Code (including changes to it or breaches of it)

I do not have powers which enable me to inspect or audit surveillance camera systems, enforce laws or otherwise impose a financial or other sanction. In contrast to my role as Biometrics Commissioner, my Surveillance Camera Commissioner functions are not 'judicial' but rather advisory in nature, and I am often called upon to give guidance and opinion on matters relating to not just the practical side of operating surveillance camera systems, but also the standards, proportionately, transparency and ethics of using such systems.

7.1 The Surveillance Camera Code of Practice

Public confidence and assurance in the accountable use of surveillance comes primarily from a framework of regulation, standards and governance. In the context of surveillance camera systems covering public spaces this framework includes the Surveillance Camera Code which the Home Secretary has a legal duty to publish[42]. Setting standards for their design and operation, the Code covers surveillance camera systems in 'public space' (although I can find no express statutory provision limiting the Code's remit to this setting) and it is for the government to designate which bodies must have regard to it. At this time those 'relevant bodies' are confined to local authorities and policing bodies[43] and the list does not include some of the largest operators of surveillance camera systems in the country, nor the government itself. The incongruity of this aspect of the legislation with the reality of surveillance camera systems being operated across England and Wales has been pointed out by my predecessor in his annual reports and I will not rehearse the arguments here. However, for any revised list *not* to include government departments in the future would surely require a very compelling case.

Acknowledged by the Court of Appeal[44] as representing part of the body of law governing what is an increasingly contentious area of activity for public bodies, the Code – and the primary legislation from which it derives its authority – is but one part of a wider framework of regulation governing the lawful, proportionate and fair use of citizen's data. That framework includes statutory guidance from the Information Commissioner and the police (see the revised Management of Police Information guidance[45]). The Code therefore represents a series of *further principles* for the specific context of public space surveillance and is only of direct legal effect in respect of policing bodies and local authorities.

---

[42] Protection of Freedoms Act 2012, s.32(1)
[43] See the Protection of Freedoms Act 2012, s. 33(5)
[44] *R (on the application of Bridges) v Chief Constable of South Wales Police and Ors, loc cit*
[45] Code of Practice on the Management of Police Information, issued by the College of Policing under s.39A of the Police Act 1996 to which chief police officers must also have regard

The Code is just one layer of regulation governing this area, with many of the issues of governance and accountability raised by surveillance being matters of wider data protection and are closely regulated by the very clear, strict and enforceable laws governing data processing, domestically and internationally. The challenge for those drafting it will be to achieve consistency both in the Code itself and – as pointed out by the Court of Appeal[46] – with the content of local policies of the relevant authorities required to have regard to it.

For my part I encourage organisations who are not relevant authorities to adopt the principles of the Code on a voluntary basis and to apply for my certification mark which allows them to visibly demonstrate that their systems are proportionate, effective, justified and transparent. The value of this scheme has been recognised by organisations such as Marks & Spencer having recently acquired full certification against the Code.

The Code was issued by the Home Secretary in 2013. Since then, technologies have evolved and become more integrated, and what was once the stuff of science fiction is now becoming a reality. Facial recognition has become a highly contentious area with limited reference to its use embedded within the Code. If the Code and the framework it supports are to remain relevant it needs to keep pace, both with technology and public concern.

I have repeated my predecessor's call, and that of many other consultees, for other organisations to be added to the list of 'relevant authorities' defined under the Act, to include the 'volume' operators of surveillance cameras in public space such as hospitals, education partnerships, transport providers and government departments. I have not succeeded in persuading ministers to extend this list. I continue to raise this with the Home Office and look forward to seeing the revised Code laid in Parliament.

7.2 Looking ahead

Paragraph 10 of the government's Declaration on Reform[47] states "We will champion innovation and harness science, engineering and technology to improve policy and services." This votive message will resonate with those leaders in policing and law enforcement who want to expand surveillance capability, adapt practices and capitalise on what is now technically possible and legally permissible. However, the developments in surveillance science, engineering and technology have been accompanied by a rapid expansion in public concern and a need for clearer legal regulation – not solely in relation to personal data – all combining to bring an important extension of public accountability.

The framework for future regulation and statutory reporting is currently under consultation by the government. On 10 September 2021, just 2 days after the consultation on proposed changes to the SC Code closed, the government launched its much wider consultation on data reform[48]. Until it was brought to my attention privately, I had been wholly unaware of the consultation or the fact that it was to contain

[46] *Bridges* at 118
[47] *Loc cit.*
[48] www.gov.uk/government/news/dcms-data-reform-consultation

a question about the transfer of my Surveillance Camera Commissioner functions to the Office of the Information Commissioner (ICO)[49].

Coming at the very end of what is a detailed document, the consultation questions (5.8.1 & 2) seek views on the government's exploration of "the potential for further simplifying the oversight framework by absorbing the functions of [the Biometrics and Surveillance Camera Commissioners'] roles into the ICO". I have published a full response to the consultation[50].

7.3 Data protection and privacy

I note that in his last annual review my predecessor said:

> "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."

In my view the relevant technical, ethical and societal considerations surrounding the deployment of surveillance camera systems by the police and others go far beyond the upholding of individual data rights and needs to be properly scrutinised beyond data protection compliance.

Not all surveillance camera-generated material qualifies as personal data for the purposes of the relevant legislative framework, but substantial areas do, and the volume of the latter can reasonably be expected to increase in the future. Whether in the form of fingerprints, DNA profiles or facial metrics, the international or cross-border processing of personal data is subject to clear regulation, safeguards and oversight. As my predecessor noted, while there are some aspects of the risks and considerations raised in this report that involve the framework for data protection, the impact of public surveillance cameras on people's lives is not confined to matters of personal data and extends to areas such as the so-called 'chilling effect' on the extent to which people feel able to hold and express opinions, meet each other and demonstrate peacefully. These are elemental constitutional entitlements which also need to be considered in the effective regulation of surveillance camera systems all of which are set out in full in my response to the consultation on the Code[51]

As to the proposal for 'absorption' into the Information Commissioner's Office (ICO) I will not rehearse my full consultation response here, but it can be summarised as follows:

To propose the 'absorption' of the Biometrics and Surveillance Camera Commissioner functions by the ICO is to misunderstand both. The evidence base for the proposal is not set out anywhere, neither are any alternatives but, if absorption is to be the answer, there are more suitable recipients for the functions, the most obvious of which is the

[49] which is why my Annual Report *qua* Biometrics Commissioner makes no reference to it: www.gov.uk/government/news/submission-of-the-biometrics-commissioners-annual-report-for-2020
[50]https://www.gov.uk/government/publications/professor-fraser-sampsons-response-to-the-surveillance-camera-code-of-practice-8-september-2021
[51] *Loc cit*

Investigatory Powers Commissioner; previous correspondence between my SCC predecessor and ministers sets this out very clearly. The new Forensic Science Regulator also has some overlap with biometrics and surveillance camera elements but as a regulator is not readily able to 'absorb' some of the statutory functions and will himself be regulating biometric databases (some owned by the government). HM Inspector of Constabulary and Fire & Rescue Services do not appear to be in a position to take on these functions.

There are some clear areas of synergy and overlap with the ICO, the most obvious being the Surveillance Camera Code and my office works closely with the ICO on related matters. For example, in May 2020 the DPIA on my website was updated in conjunction with the ICO to assist organisations comply with their data protection and PoFA responsibilities when operating surveillance camera systems. Many of the legal issues arising within surveillance activity engage with more generic GPDR issues and even the legal challenge to the Chief Constable of South Wales Police was, in many ways, a 'data protection' case arising in the context of surveillance camera technology, while the ICO has intervened in matters such as ANPR[52]. And the international exchange of biometric data is covered principally by schedule 14 to the DPA 2018 giving the ICO express legal responsibility (although this area is already complex and controversial even for several independent commissioners acting jointly).

One immediate simplification that would flow from the ICO's absorption of the Biometrics and Surveillance Camera Commissioner's functions would come from the Information Commissioner's UK-wide jurisdiction. Under the current arrangements there is a need for the UK government to pass *additional* secondary legislation[53] to ensure that biometric data obtained in England, Wales or Northern Ireland but used by police and law enforcement bodies in Scotland, comes under the Scottish Biometrics Commissioner's functions. As the ICO already has UK-wide functions over such data the need for this secondary legislation would be obviated, thereby simplifying the regulatory framework.

Nevertheless, the majority of my time in the Surveillance Camera Commissioner arena is spent dealing with non-data protection issues such as the erosion of elemental human rights like freedom of assembly and speech, promotion of the state's positive articles 2 & 3 obligations and the ethical issues arising from surveillance including the conduct of Chinese technology companies (which concerns arise from informed internal partner agencies as well as external commentators).

Given the current level of public concern in the areas of facial recognition and surveillance, simplifying oversight arrangements at the cost of dilution seems counterintuitive – most people are clamouring for *better* regulation of these developments, especially in schools and large public areas such as transport hubs, and it is unclear how or why the ICO's 'absorption' would deliver that.

I continue to have regular meetings with the Home Office about the progress of both consultations and relevant stakeholder engagement. Given the timescales that would necessarily attend any amendments to primary legislation in this area I do not expect to see any substantive changes during my term of office which ends in February 2023.

[52] https://www.independent.co.uk/news/uk/crime/royston-ring-steel-data-watchdog-warns-police-surveillance-scheme-rural-hertfordshire-town-unlawful-8730811.html
[53] See the Scottish Biometrics Commissioner Act 2020 (Consequential Provisions) Order [Draft] 2021

Resources

For the reporting year, the resource allocated to my office was an annual budget of £305,000. My predecessor in his last annual report provided a detailed outline of the resources he believed were required to be fully supported in this role[54]. Having been in post for 7 months, I agree with his assessment that the government should dedicate greater resource to this office, given the proliferation of surveillance camera systems in use and the level of public concern about their use. However, notwithstanding requests for additional resource, the budget has remained static, and the failure to backfill vacant posts following people leaving the department and being on maternity leave has resulted in the office operating at a 50% staffing level for much of the reporting year.

There was also a 3-month period from December 2020 to February 2021 when no Commissioner was in post. The public appointments process took place during the COVID-19 pandemic and, as my predecessor's term had already been extended on several occasions, he left the role with no named successor. I know that this was a difficult time for my office to navigate, with some work processes having to be paused owing to restrictions on Home Office employees being able to act in the absence of a commissioner. The backlogs that inevitably built up placed even greater strain on an already diminished office.

The Office of the Surveillance Camera Commissioner has now merged with the Office of the Biometrics Commissioner and the budgets have been combined to total £607,000, although both offices remain significantly under-resourced. In carrying out my functions I am almost entirely dependent on staff provided to me by the Home Office and I have been hugely impressed with their capability, flexibility and resilience during a period of significant uncertainty and demand. I hope in my next Annual Report to be able to provide assurance of greater stability and capacity within the combined team.

[54] https://www.gov.uk/government/publications/surveillance-camera-commissioner-annual-report-2018-to-2019

E02682343
978-1-5286-2965-2