Response to the Government's
Statutory Consultation on the Surveillance Camera Code under s.29(5)(e)

Abstract

The world of surveillance has shifted and the regulation surrounding it must reflect such changes if it is to remain relevant. The scope of the review is very modest and subsequently the proposed amendments to the Code are relatively minor.

The acid test for the revised Code 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).

Introduction

1. Having been acknowledged by the Court of Appeal[1] as representing part of the body of law governing what is an increasingly contentious area of activity for public bodies, the Surveillance Camera Code of Practice (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[2] currently under consultation). 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 which are currently the only 'relevant authorities' designated for the purposes of the legislation[3].

2. The Code is just one layer of regulation governing this area, many of the issues of governance and accountability raised by surveillance are 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[4] - with the content of local policies of the relevant authorities required to have regard to it.

3. On taking up my appointment as Biometrics and Surveillance Camera Commissioner in March 2021, I and my office were in continuing dialogue with the Home Office about a proposed revision of the Code. My predecessor, Tony Porter, had been very active in seeking a revision of the Code and had proposed a number of amendments to the statutory regime itself[5]. I too suggested some changes to the Code, however it was made clear that the scope of any formal revision would, at this stage, exclude any structural alteration or amendment of the Code's principles and does not include a review of the list of relevant authorities. It is no surprise then that the extent of proposed changes within the draft

[1] *R (on the application of Bridges) v Chief Constable of South Wales Police and Ors* [2020] EWCA Civ 1058

[2] 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

[3] See the Protection of Freedoms Act 2012, s. 33(5)

[4] *Bridges* at 118

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502893/Draft_Review_FINAL.pdf

that has been circulated for consultation are modest and have been received as such[6]. I have not rehearsed my original suggestions here, however they are available through my office.

The Changing Surveillance Context

4. Since the Code was first published almost a decade ago the field of surveillance camera systems has changed dramatically. Before looking at the specific issues in this consultation it is perhaps worth noting that when the current Code was published Edward Snowden was still a contractor for the NSA[7], and only 15 chief constables and 5 police and crime commissioners responded to the first statutory consultation on its content[8].

5. The relevant legislation[9] was new and the existence of a statutory Code very much reflected the Government's position that "further regulation of CCTV and other surveillance cameras will be an incremental process which is largely self-regulatory, builds on the foundation of existing legislation, and starts with getting the basics right"[10]".

6. Today those 'basics' have shifted significantly and, along with them, the legitimate expectations of the industry, the operator and, most importantly, the citizen. Getting them right will require a correlative shift. In understanding how and where the shift is needed, it is helpful to look at the surveillance realities which the Code purports to address, from three interlocking perspectives:

    1) the technologically possible (what can be done),
    2) the legally permissible (what must/must not be done) and
    3) the societally acceptable (what communities will tolerate and support).

Technologically possible (what can be done)

7. The Code was written both at and for a time when a CCTV camera mounted on a local authority van was showcased as representing the "latest high-tech surveillance equipment"[11]. The principles still hold good and the 'basics' have evolved to meet the requirements of a scenario close to that envisaged by Accenture in 2018[12] as representing a Tier 1 state, whereby we have a mass public safety ecosystem relying primarily on CCTV used retroactively by the police to understand "what happened".

8. Increased technology has been accompanied by increased coverage in public surveillance. When measured by the number of cameras to people, London has recently[13] been ranked the 3rd most surveilled city on Earth (having an estimated 691,000 cameras for 9,425,622 people = 73.31 cameras per 1,000 population), while, in cameras per square mile, it comes second (691,000 cameras for 607 square miles = 1,138.48 cameras per square mile). When mobile camera platforms covering public spaces such as drones are included, and privately owned and operated cameras are factored in, there is no reliable figure. When the Code was first published however, the BSIA put the ratio of private to

[6] https://www.bbc.co.uk/news/technology-58206586
[7] https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance accessed 24 August 2021
[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/206693/surveillance-camera-code-of-practice-responses-revised-web.pdf accessed 24 August 2021
[9] The Protection of Freedoms Act 2012
[10] *Loc cit* p.12
[11] https://www.infologue.com/company/ocs-invests-in-high-tech-cctv-vehicle-for-london-borough-of-lambeth/ accessed 25 August 2021
[12] "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
[13] https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ accessed 25 Aug 2021

public cameras at 70:1[14]; it is a reasonable hypothesis that this relative imbalance will have increased since.

9. Expansion in capability of privately owned cameras has been accompanied by a corresponding increase in the sharing of private operators' images with the police[15], whether of the citizen's own volition, by commercial agreement, or in response to the now ubiquitous police appeals for dashcam, GoPro or other footage[16].

10. When it required human monitoring and analysis, all this newly enabled aggregated surveillance data had limited practical use: there is simply too much of it. But technological advances in video analytics and systems for combining, categorising and editing these datasets now allow very significant uses of the product of this new surveillance capability. Taken together, these technological advances will allow commercial businesses and householders alike to 'plug' their cameras into police and local authority networks, while the addition of artificial intelligence has been identified as "investing closed-circuit television, or CCTV, networks with the power for total public surveillance"[17]. The rapid evolution towards what has been called *omniveillance*[18] means we are already moving up from the final features in Accenture's Tier 1 scenario above, where "data is typically stored in silos, making it difficult to create a broader and more comprehensive picture of a particular situation but some cities begin to leverage emerging technologies to manage mundane public safety tasks."[19] Tier 2 is "expected to arrive by 2025" and is characterised by "a mass real-time-oriented public safety ecosystem where through AI, police can see the unseeable". In less than four years' time, Accenture's estimate is that 70% of security surveillance cameras will be supplied with on-device real-time monitoring and analytics functions within the camera (compared with less than 5% in 2018). This will allow governments and the police to "crowdsource video data from businesses and public institutions (such as schools and hospitals) to augment their current CCTV feeds and add AI capabilities that enable them to track and analyse footage in real time to identify anomalies and threats[20]".

11. This significant increase in the technologically possible (what can be done) drives changes in the purposes for which that surveillance technology can be used, bringing in the second and third perspectives: the **legally permissible** (what must/must not be done) and the **societally acceptable** (what communities will tolerate and support).

Legally permissible (what must/must not be done)

12. As with the technology, at the time the Code was written the legal and regulatory landscape was also very different. In order to understand that landscape in the context of surveillance cameras the legal issues can be divided into data protection and non-data protection issues.

Data Protection

---

[14] https://www.protectorsecurity.co.uk/news/just-1-in-70-cctv-cameras-are-state-owned/

[15] https://www.theguardian.com/commentisfree/2021/apr/05/tech-police-surveillance-smart-home-devices accessed 28 August 2021

[16] Whether the increased police reliance on citizen-generated data will create a dependency (and therefore a risk) for the future is not yet measurable but the *de facto* agency of the citizen acting under direction of the police when using their own personal devices may become a *de jure* extension of a 'relevant authority' and may thus be caught by the Code.

[17] Michael Kwett, *The Intercept https://muckrack.com/michael-kwet/articles* accessed 25 August 2021

[18] Blackman, J., (2008) Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet, 49 Santa Clara L. Rev. 313

[19] *Ibid*

[2020] *Ibid*

13. The law has long recognised that some data by their very nature carry specific sensitivity and risk for the person to whom they relate and can compromise, not just the subject's privacy, family life[21] and correspondence but in some cases their very identity[22]. The laws regulating the processing of those data generally have evolved quickly in response to technological possibility.

14. The framework for data protection changed significantly in 2016 with the passing of the General Data Protection Regulation,[23] the key legal instrument regulating data protection in EU Member States, which came into effect in May 2018. This instrument introduced a number of new rights and expressly refers[24] to the 'state of the art' when assessing and implementing appropriate technical and organisational measures. Further legal adjustments have been made to the legislation to take account of technological advances such as automated decision-making,[25] reflecting how the legal threshold (permissibility) will necessarily shift in response to the technological (possibility).

15. Data protection and the international regulatory framework – including the specific context of policing and law enforcement[26] - are the responsibility of the Information Commissioner who is the national data protection authority for the UK[27]. A substantial amount of the data processed by surveillance camera systems qualifies as 'personal data' and its lawful processing (which includes storage and sharing) is principally a matter for the Information Commissioner's Office (ICO). As surveillance camera systems are often designed and deployed to identify (directly or indirectly) a living person by reference to an identifying feature, location data, or to one or more factors specific to their physical identity, physiological, mental, economic, cultural or social identity[28], the concept of *personal information* is central to the legal framework governing this area and the law has adapted in response to technological capability. 'Personal information' can include CCTV footage[29], personal images[30], fingerprints and DNA samples[31], a person's home address [32] and IP address[33]. Therefore, the lawful use of new surveillance technology such as live facial recognition[34] or the use of the Automated Number Plate Recognition (ANPR) system in England[35] or other parts of the UK,[36] will generally involve broader data protection rights and remedies rather than requiring any 'surveillance camera-specific' laws. The main source of protection for information engaging relevant human rights such as the right to respect for private and family life[37] engaged by this aspect of surveillance is the Data Protection Act 2018 and its established principles, Part 3 of which directly addresses the specific context and

---

[21] Guide on Article 8 of the European Convention on Human rights https://www.echr.coe.int/documents/guide_art_8_eng.pdf

[22] *Axel Springer AG v Germany* 39954/08

[23] The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)

[24] Art 25

[25] Convention 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe) https://rm.coe.int/1680078b37

[26] Directive EU2016/680 which is given domestic effect in Part 3 of the Data Protection Act 2018

[27] https://ico.org.uk/about-the-ico/what-we-do/

[28] All features of the definition in the General Data Protection Regulation European Union no. 2016/679.

[29] *Peck v UK* 44647/98

[30] *von Hannover v Germany (no 2)* 40660/08

[31] The storing of which amounts to an interference with subject's private life under the European Convention on Human Rights, Article 8 (*S. and Marper v UK loc cit*.

[32] *Alkaya v Turkey* 42811/06.

[33] *Benedik v Slovenia* 62357/14

[34] See the grounds of challenge and appeal in *R (on the application of Bridges) v Chief Constable of South Wales Police and Ors* [2020] EWCA Civ 1058, many of which were determined on the application of generic data protection or public equality duty matters.

[35] https://www.independent.co.uk/news/uk/crime/royston-ring-steel-data-watchdog-warns-police-surveillance-scheme-rural-hertfordshire-town-unlawful-8730811.html

[36] https://www.scotsman.com/news/transport/police-delete-half-billion-records-drivers-plates-1445560 accessed 26 August 2021

[37] As protected by the European Convention for the Protection of Human Rights and Fundamental Freedoms article 8

operational requirements of policing. The Code is consistent with these principles and provides a gloss on the much broader statutory framework governing the 'processing' of personal data[38].

16. As technology advances and surveillance camera systems are adapted to collate more information from which a person can be identified, it will be essential for the regulatory arrangements as a whole to advance and adapt accordingly, providing a clear, consistent, and comprehensive framework.

17. To this end, the ICO provides advice and guidance on all data protection-related matters and the conduct of data protection impact assessments, including some that involve the use of surveillance camera technology[39], and works closely with the Surveillance Camera Commissioner; both produce guidance that is cross-referenced, including the existing Code and the Information Commissioner is also a statutory consultee for any proposed revision of the Code.[40]

Non-Data Protection Issues

18. Not all legal considerations governing what must/must not be done with surveillance cameras are data protection issues. For example, the presence – or even the perceived presence – of a police surveillance camera may discourage people from meeting, expressing views or exercising their right to protest peacefully.[41] The potential impact on the fundamental human rights of the citizen and the so-called "chilling effect"[42] are central to the lawful (and acceptable – see below) operation of surveillance cameras[43]. The ability of mass surveillance to interfere with the most elemental of human rights is well documented[44], and that ability and potential impact has probably increased since the COVID-19 pandemic.[45]

19. Moreover, whereas new technology can allow greater specificity – and therefore reliability – in identifying an individual and is therefore more likely to involve 'personal data' as defined above, some analytics used to match datasets or extrapolate conclusions from trends and patterns in Big Data *without* revealing the identity of a person may not come within the legal framework for data protection[46].

20. At the same time, there are surveillance-related obligations on the state that go beyond data protection. Obligations that may include the reliability and product of surveillance camera systems used in a criminal investigation or prosecution, for example. These would fall within the remit of the new Forensic Science Regulator[47] (who, as a new legal entity, is not a statutory consultee for the Code). The state also has *positive* human rights obligations to take practical and effective measures to protect

[38] Which includes storing, sharing and deleting

[39] See https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf; and https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf accessed 28 August 2021

[40] Protection of Freedoms Act 2012, s.29(5)(c)

[41] As protected by the European Convention for the Protection of Human Rights and Fundamental Freedoms articles 9-11

[42] https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf accessed 26 August 2021

[43]See e.g. Murray, Fussey, McGregor & Sunkin https://www.proquest.com/openview/9201da92e00f8c776ea70d6655071948/1?pq-origsite=gscholar&cbl=286204accessed 26 August 2021

[44] See e.g. *Big Brother watch v UK* 58170/13, 62322/14 and 24969/15*;* Rusinova (2021) Privacy and the legalisation of mass surveillance: in search of a second wind for international human rights law, The International Journal of Human Rights, DOI: 10.1080/13642987.2021.1961754; *Roth & Wang (2019) https://www.hrw.org/news/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state* ;Watt (2017) 'The right to privacy and the future of mass surveillance', The International Journal of Human Rights, 21:7, 773-799, DOI: 10.1080/13642987.2017.1298091

[45] https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/ accessed 26 August 2021

[46] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[47] See the Forensic Science Regulator Act 2021

its citizens from certain types of harm (death, torture, inhumane and degrading treatment)[48]. Often overlooked in the public debate about the use of available technology, these positive obligations would include due consideration of deploying available technology such as facial recognition surveillance cameras in the prevention of certain types of serious criminality. It is clear that, within the boundaries of this positive obligation, the police have a legal duty to use all means reasonably available to them[49] and those means are becoming increasingly available as technology advances.

21. Finally, it is important to note the regulatory regime for the *covert* use of surveillance capabilities and technologies such as communications intercepts and bulk data acquisition. The Investigatory Powers Commissioner's Office (IPCO) has statutory responsibility[50] for the independent oversight of the use of the most intrusive surveillance powers. Working very closely with the Office for Communications Data Authorisations (OCDA) the IPCO publishes annual reports, the latest of which illustrates the work of the Commissioner and the judicial commissioners who assist him[51] in what has been recognised by the UN High Commissioner for Human Rights office as a leading model for surveillance oversight.[52]

Societally acceptable (what communities will tolerate and support).

22. The brief snapshot of the legal landscape not only reflects *how* the law has changed since the Code was first published, but also *why*. Some of the changes have been a direct response to what is technologically possible, such as the regulation of automated decision making. But that legal landscape also reflects *the response of citizens* to their evolving surveillance environment. To an extent, all new legislation in a democracy is a product of the will of the electorate but the law in relation to data protection, the retention and use of biometrics and the protection of freedoms in an era of burgeoning surveillance has been almost entirely the product of litigation. Many of the changes to the law in this area have been impelled by individual legal challenges brought by, or on behalf of, the citizen[53].

23. Which gives rise to the third perspective. The future of surveillance is being shaped in the area of what communities are prepared to tolerate and support, not just in England and Wales, but around the world. Societal acceptability here goes beyond notions of 'consent' (informed, contingent, conditional, express, implied, or otherwise) as relied upon in the current Code. Acceptability in this context is a wider democratic construct made up of ethics, mores and legitimate expectations. It can be peculiar to specific communities or generally applicable and can be seen in some of the many global reactions to technically possible and legally permissible surveillance developments such as Live Facial Recognition[54]. It can also be seen in challenges to police use of AI and automated decision-making technology in mobile phone tracking via cell-site simulators ('Stingrays")[55], Automated Licence/Number Plate Readers, Toll Payment Readers, Shot Spotters (acoustic devices), X-Ray Vans and

---

[48] See e.g. *Valiuliané v Lithuania* 33234/07; *Rantsev v Cyprus & Russia* 25965/04; *BV v Belgium* 61030/08

[49] *Commissioner of Police of the Metropolis v DSD and Another* [2018] UKSC 11

[50] Part 8 of the Investigatory Powers Act 2016

[51] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf

[52] Although with reservations around the legislative provisions that require authorisation and oversight to be undertaken in the same office- see https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23297 accessed 2 September 2021

[53] See for example *S & Marper* 30562/04; *R (on the application of GC & C) v Commissioner of Police for the Metropolis* [2011] UKSC 21; *Digital Rights Ireland & Seitlinger* C-293/12; *Maximillian Schrems v Data Protection Commissioner Ireland* ("Schrems I") C-362/14; *Tele2 Sverige* C-203/15; *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12; *Data Protection Commissioner v Facebook Ireland Ltd. & Maximillian Schrems* C-311/18 (Schrems II") .

[54] MPS – 90% error rate (Dodd, V 2018 https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure – accessed 26 August 2021; Orlando Police Department abandoned use of Amazon Rekognition software as a result of technical issues - https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended accessed 26 August 2021

[55] Joseph, G 2018, https://www.bloomberg.com/news/articles/2016-10-18/u-s-police-cellphone-surveillance-by-stingray-mapped, 18 October, accessed 26 August 2021

"Surveillance-Capable Lightbulbs"[56] whereby pressure from citizens has sought to change the law and *pre-empt* the use of future technological capability.

24. 'Societal acceptability' essentially acts as a democratic brake on the technological exuberance that drives innovation, and in the field of surveillance there is a marked movement towards the citizen resisting what can be done technologically and legally. While access to effective legal remedy is itself a fundamental human right[57], the recourse to litigation referenced above is not necessarily the most efficient or effective way of asserting democratic accountability. The 'relevant authorities' covered by the Code already have well-established mechanisms for public consultation, scrutiny, challenge, audit and complaints. In the setting of policing, the role of elected local policing bodies[58] here is critical as they were established expressly to hold their local police to account on behalf of their communities. One would therefore expect them to be closely sighted on the attitude towards surveillance camera systems – which range from CCTV, ANPR and body worn devices, as well as drones and other airborne cameras used by, for example, the National Police Air Service. The extent to which these relevant authorities comply with the existing Code is assessed by my office biennially[59]. Key findings from the latest LA survey in 2020, were: that 50% of local authorities responded, and it was found that 6,000 systems and 80,000 cameras are in operation across 183 LAs, most of which are CCTV systems, but BWV and dash cams are also in use. Only one LA said they didn't operate any surveillance cameras. The majority of main town centres schemes can demonstrate compliance with the Code through completion of a Self-Assessment Tool, however away from these main schemes, completion of a SAT varied from 26%-58% (LAs were not asked if compliance was demonstrated via other means). Key findings from the latest police survey in 2019, were: that 100% of forces responded (43 police forces, British Transport Police, Civil Nuclear Constabulary and the Ministry of Defence Police), and the majority of forces are operating CCTV, ANPR, Body-Worn Video and drones. Where forces are operating surveillance camera systems, compliance with the Code ranges from 56%-100% and completion of a SAT to demonstrate compliance ranges from 60%-86%.

25. Rising public concern at the use of surveillance camera systems will only increase the importance of this locally accountable consultation and communication in the future. In their analysis of the competing issues Accenture stated[60] that "public input and oversight are necessary to ensure that video public safety systems are designed to prevent misuse and abuse. Members of communities considering such a system should participate in the decision-making process to build trust and tailor public safety processes to the community's needs and circumstances". This is corroborated by experience in the United States where the backlash against the deployment of some surveillance technology by the police has been among the starkest. In relation to one such system, Amazon Rekognition, a lawyer for the American Civil Liberties Union said "this failed pilot program demonstrates precisely why surveillance decisions should be made by the public through their elected leaders, and not by corporations secretly lobbying police officials to deploy dangerous systems against the public[61]", while the IBM CEO is reported as saying "we believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies[62]".

---

[56] ACLU Report "Community Control Over Police Surveillance" Technology 101 pp 3-6

[57] See art 13 European Convention on the Protection of Human Rights

[58] Police and crime commissioners and deputy mayors for policing and crime under the Police Reform and Social Responsibility Act 2011

[59] https://videosurveillance.blog.gov.uk/2020/10/20/survey-of-local-authorities-compliance-with-the-protection-of-freedoms-act-2012/

[60] *Loc cit.* p14

[61] Cagle (2019) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new?redirect=blog/amazon-teams-law-enforcement-deploy-dangerous-new-facial-recognition-technology accessed 28 August 2021.

[62] *Ibid*

26. In sum, since the Code was first published the capability, legality and acceptability of surveillance camera technology has undergone transformational change. It is against that backdrop that the proposed changes will need to be viewed.

The Proposed Changes

27. In its response to the first consultation, the Government undertook to review 'the operation and impact of the code' in 2015, and to include 'the extent to which system operators are adopting the code voluntarily and demonstrating greater transparency'. This review was to be informed by advice from the Surveillance Camera Commissioner and followed by statutory consultation *on the extent of those listed under s.33 as relevant authorities, placing others under a duty to have regard to the code if necessary*[63]. I am advised that this review and consultation did not take place.

28. The current consultation is to be limited to statutory consultees expressly named in the legislation[64]. I have encouraged responses from anyone having an interest in this area and my office has been asked to coordinate any such responses; we will pass these to the Home Office in the form in which we receive them.

29. Working within these parameters, I and my team have discussed the proposed changes in the consultation draft and have helped shape the wording, to reduce the volume and focusing the Code on enabling relevant authorities to operate surveillance camera systems in a lawful, proportionate and accountable way.

30. I agree with my predecessor's position[65] that the list of 'relevant authorities' ought to be reviewed in light of the expansion of surveillance camera systems covering public space, the increased public awareness of such surveillance and the attendant sensitivities outlined earlier in this response.

31. In its response to the first consultation the Government also stated that "*the code is intended to be an important step in an incremental approach to regulation that will help reassure the public that their civil liberties are being respected and enable them to challenge a system operator wherever they have concerns. It should also encourage the wider adoption of good practice where surveillance is necessary and proportionate*"[66] [emphasis added]. In light of this intention and our collective experience since it was expressed, the Government should, as an absolute minimum, voluntarily adopt the Code across its estate.

32. On 15 July 2021 I wrote to ministers[67] regarding the risks and considerations of surveillance camera systems under extra-territorial ownership and I would ask that the content of that letter be considered as part of my formal response to this consultation. I believe that the Code ought to provide clear direction and guidance to relevant authorities as operators and purchasers of surveillance camera systems where those systems are supplied by companies under extra-territorial ownership, such direction and guidance addressing in particular:

---

[63] *Loc cit* p.9

[64] S.29(5)(a)-(f)

[65] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502893/Draft_Review_FINAL.pdf

[66] *Loc cit* P6

[67] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003046/BSCC_Letter_to_Baroness_Williams_-_Surveillance_Camera_Systems_Under_Extra-Territorial_Ownership_July.pdf

1. the risks arising from data security, cyber-attack and 'function creep'.
2. the level of appropriate consideration where there is reason to believe that suppliers or manufacturers have been associated with breaches of international law or human rights abuses[68] and
3. the relative weight that should be given to the economic considerations that the other areas set out above when conducting public procurement or contract management exercises.

33. Immediately before this consultation I exchanged correspondence with a surveillance camera system supplier following a request for advice and guidance arising from the issues at 31.2.[69] The reported uses of technology as raised by the Commons Foreign Affairs Committee earlier this year[70] represent a real-life manifestation of people's worst fears in the dystopian deployment of surveillance camera systems. If the Code is to produce socially responsible surveillance of public places, public reassurance and the adoption of good practice, then it also needs to cover the ethical aspects of technological exploitation and the trading practices of surveillance companies themselves. Having committed itself to ensuring that its work and relationships are underpinned by respect, compassion and courage[71], the Home Office has to that extent already subscribed to the necessary values, it now needs to apply those values to addressing the urgent concerns expressed in the Foreign Affairs Committee report. Moreover, an ethical and socially responsible approach is surely a legitimate expectation for the citizen where surveillance systems are being bought with public money. In this context it is worth noting the Declaration on Government Reform[72], signed by the Prime Minister and Cabinet Secretary on 15 June 2021, which avows to "hold those with whom we contract more rigorously to account" and to "draw on insights and learnings from other countries to help inform actions we take at home"; both avowals are of direct relevance to this pressing issue.

34. I would also encourage the Government to incorporate the revised Code into the licensing requirements for drone pilots as regulated by the Civil Aviation Authority, as the use of drone-borne surveillance cameras is likely to increase exponentially in the next few years.

35. Finally, given his statutory functions which will regulate 'activity relating to the application of scientific methods for purposes relating to the detection or investigation of crime in England and Wales or the preparation, analysis or presentation of evidence in criminal proceedings in England and Wales'[73], I believe that the Forensic Science Regulator ought to be listed as a statutory consultee for the purposes of the Code and its revision, as the product of surveillance cameras falls squarely within that definition.

Conclusion

"We will champion innovation and harness science, engineering and technology to improve policy and services." Paragraph 10 of the Government's Declaration on Reform[74] will resonate with those leaders in policing and law enforcement who want to expand surveillance capability, adapt practices and capitalise on

[68] See e.g. paras 58-59 https://committees.parliament.uk/committee/78/foreign-affairs-committee/news/156425/foreign-affairs-committee-publish-report-never-again-the-uks-responsibility-to-act-on-atrocities-in-xinjiang-and-beyond/; accessed 27 August 2021

[69] https://www.gov.uk/government/publications/never-again-the-uks-responsibility-to-act-on-atrocities-in-xinjiang-and-beyond

[70] *Loc cit*

[71] https://www.gov.uk/government/publications/home-office-outcome-delivery-plan/home-office-outcome-delivery-plan-2021-to-2022

[72] _https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993902/FINAL_Declaration_on_Government_Reform.pdf accessed 28 August 2021

[73] The Forensic Science Regulator Act 2021 s.11

[74] *Loc cit.*

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.

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 are such that their responsibilities ought to be combined or streamlined in the future. This will ultimately be a matter for others. 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 demonising it irrational. It is clear that the areas of surveillance covered by the Code are heavily and iteratively regulated as described above. There are other areas such as commercial and individual private use of new surveillance technology that fall outside any of the regulatory frameworks[75]. If the Code and other legislative instruments cover the 'regulated knowns', what is covering the development of the 'unregulated unknowns'? This is a fast-evolving area and the evidence is elusive, but it would be slightly 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[76], that they can only be acceptably carried out under licence – perhaps akin to the regulatory arrangements for human fertilisation and embryology. 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[77]", a future in which "deep learning enables the system to become more knowledgeable and, as a result, more accurate[78]" we need *as a minimum* a single set of clear principles by which those operating surveillance camera systems will be held to account, transparently and auditably. The acid test for the revised Code 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).

[75]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

[76] 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

[77] Accenture's Tier 3

[78] *Ibid*