CRISP
CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

INDEPENDENT REPORT ON CHANGES TO THE FUNCTIONS OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER ARISING FROM THE DATA PROTECTION AND DIGITAL INFORMATION (No.2) BILL

6 October 2023

Professor Pete Fussey
Professor William Webster

CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
ANPR	Automated Number Plate Recognition
BC	Biometrics Commissioner
BSIA	British Security Industry Association
BSCC	Biometrics and Surveillance Camera Commissioner
CCTV	Closed Circuit Television
DASA	Defence and Security Accelerator
DCMS	Department for Digital, Culture, Media and Sport
DNA	Deoxyribonucleic Acid
DPDI	Data Protection and Digital Information Bill
DSIT	Department for Science, Innovation and Technology
EHRC	Equality and Human Rights Commission
FINDS	Forensic Information Database
FRT	Facial Recognition Technology
FSR	Forensic Science Regulator
GDPR	(European Union) General Data Protection Regulation
IAG	Independent Advisory Group for Automated Number Plate Recognition
ICO	Information Commissioners Office
IPA	Investigatory Powers Act 2016
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioner's Office
LFR	Live Facial Recognition
LGA	Local Government Association
NASPLE	National ANPR Standards for Policing and Law Enforcement
NPCC	National Police Chiefs' Council
NSD	National Security Determinations
OBSCC	Office of the Biometrics and Surveillance Camera Commissioner
PACE	Police and Criminal Evidence Act 1984
POFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SBC	Scottish Biometrics Commissioner
SCC	Surveillance Camera Commissioner
SCCoP	Surveillance Camera Code of Practice
SSAIB	Security Systems and Alarms Inspection Board
UK	United Kingdom

EXECUTIVE SUMMARY

Introduction

Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. At the time of writing, deployments of technologically advanced biometric surveillance techniques, including facial recognition technology, are accelerating at an unparalleled rate. The Minister of State for Crime, Policing and Fire has expressed clear ambitions to embed facial recognition technology into UK law enforcement, radically increase the reference database of comparable images, and in August 2023 the government announced a scheme to fund enhancements in the capability and feasibility for law enforcement and other security uses in the UK. Such developments raise the importance of meaningful oversight and regulation.

The Government introduced The Digital Information and Data Protection (no.2) Bill) (DPDI Bill) into Parliament during 2023 with the stated aims of simplifying, bringing clarity and future proofing the oversight of surveillance cameras and biometric materials. Part V of the DPDI Bill seeks to remove the obligation on the Government to publish a Surveillance Camera Code of Practice (SCCoP) and consequently remove the post of the Surveillance Camera Commissioner (SCC) whose functions are derivative from the SCCoP. The Bill also proposes to amend s.20 of the Protection of Freedoms Act (POFA) 2012 by abolishing the role of the Biometrics Commissioner (BC). These two Commissioner roles were created separately under the POFA with one person appointed to both roles in 2021. This merger created the role of the Biometrics and Surveillance Camera Commissioner (BSCC). The Bill proposes to delete all BSCC surveillance camera-related oversight activities and mechanisms and all but some selected biometric casework activities. Specifically, the Bill makes provision for the transfer of the BSCCs judicial functions covering Police and Criminal Evidence Act (PACE) 1984 s63G provisions and National Security Determinations (NSD) casework covering the oversight and review of biometric data retention. A significant number of other activities that arise from the fulfilment of statutory duties placed on the BSCC and integrated into everyday public surveillance practice will also disappear.

It should be noted that the Bill also proposes substantial changes to the ways in which data processes will be regulated in the future, with significant structural and procedural changes to the existing data protection regulatory regime in the UK.

This report offers a detailed analysis of these changes. The purpose is to analyse how the oversight of surveillance cameras and biometric materials will change under provision in the Bill, and identify the gaps that are likely to arise. Both authors are academic professors specialising in the oversight and management of surveillance and both have held professional roles leading designated strands of the BSCC National Strategy, the principal mechanism supporting the BSCC role. The report draws on evidence gathered through consultation and qualitative interviews with leading practitioners and experts in the field. This includes representatives from law enforcement holding national strategy roles addressing surveillance, national-level professional organisations representing surveillance camera operators, industry representatives, national regulators and internationally recognised academic experts holding decades of professional experience analysing surveillance oversight. The analysis was commissioned by the BSCC but report itself and the authors' analysis is wholly independent.

Rationale for the proposed changes

It is widely accepted that current arrangements for oversight for public surveillance and biometric techniques are complex and would benefit from greater clarity. The Government has advanced several arguments for this change:

a. Simplification. It is widely accepted that existing oversight of complex surveillance practices is fragmented and requires simplification.
b. A belief in sufficient existing oversight coverage. The stated Government position relies on the argument that sufficient oversight of both public surveillance and biometric materials already exists elsewhere. The ICO, Equality and Human Rights Commission, His Majesty's Inspector of Constabularies and Fire and Rescue Services, and the Home Office Forensic Information Database (FINDS) Board (formerly called the National DNA Database Strategy Board) are all cited as other venues providing similar oversight. The government further argues that such claimed duplication of oversight creates difficulties for policing, local authorities and other public agencies seeking to enhance public safety.
c. Government documentation also points to the intention of adopting a 'principles-based approach' to address the problem of highly specified technology-focused or otherwise piecemeal approach to legislation which can become quickly outdated.

The role and activities of the Biometrics and Surveillance Camera Commissioner and oversight gaps arising from the abolition of the role.
The oversight of public space surveillance cameras is realised through statutory functions laid out in POFA and realised through the BSCC. The BSCC plays an important role in the governance and use of biometric materials and surveillance camera technologies by public agencies. The key roles of the Commissioner are defined in legislation and are underpinned by both statutory and non-statutory activities.

Regarding the Surveillance Camera Commissioner (e.g. ostensibly non-biometric) functions, section 34 POFA places responsibility on the Commissioner to *"(a) encourag[e] compliance with the [Government] surveillance camera code, (b) revie[w] the operation of the code, and (c) provid[e] advice about the code (including changes to it or breaches of it)"*. The key purpose behind the legislation is to drive up standards, ensure 'best practice' and provide reassurance to the public that cameras are being used appropriately and within the law. The BSCC role also allows considerable latitude for considering emerging technologies.

The DPDI Bill proposes to remove the legislative need for the Government to publish a SCCoP, which offers governance coverage far beyond data-related issues. This *would result in* the abolition of all SCC-related functions. Surveillance users regard the SCCoP and associated guidance as touchstone documents. Abolishing this guidance and associated mechanisms designed to support compliance creates vulnerabilities for users of these technologies and for the rights of individuals subjected to them. Furthermore, erasing existing guidance and support mechanisms for compliance are likely to undermine ambitions for the simplification of oversight.

Under POFA the Surveillance Camera Commissioner and Biometrics Commissioner are obliged to produce an annual report to be laid before Parliament. Since 2021 the two separate reporting obligations have been combined into the same publication. Annual reporting provides a measure of transparency over how public surveillance tools are used and how biometric materials are overseen. Such reports also confer accountability and work towards enhancing public confidence in these activities. The DPDI Bill proposes to abolish the requirement to produce such reporting. This removes another element of transparency and accountability in an area of significant and growing public concern.

Deleting the SCCoP would have a cascading impact on the non-statutory functions and activities of the BSCC. This is important because delivering the BSCC statutory obligations is contingent on the following non-statutory activities. These activities are held in high regard by practitioners and have proved effective in driving up the standards of procurement, use and legitimacy of public surveillance cameras. The non-statutory functions and activities that will be lost include:

a. *The National Surveillance Camera Strategy for England and Wales*. The statutory obligation under POFA S34(a) to encourage compliance with the Government SCCoP is delivered through the National Strategy. It therefore constitutes an important vehicle in delivering the BSCC statutory functions. In addition, a key function of the National Strategy is to engage stakeholders and the general public to build awareness about the use of surveillance cameras in society. This is particularly important at a time when trust and confidence in the police and other public institutions is particularly challenged.
b. *The Certification Scheme and Self-Assessment Tool* is a mechanism for camera operators to demonstrate compliance with the SCCoP and become certified by the BSCC. This initiative is popular among practitioners in providing clarity to their activities and in raising standards.
c. *The Surveillance Camera Standards Group* defines minimum technical specifications and standards necessary in a for surveillance camera systems that develop in sophistication and technical ability.
d. *The Buyer's Toolkit* comprises a guide that sets out detailed procurement guidelines for those responsible for purchasing and installing surveillance camera equipment and systems.
e. *Training*. The BSCC has also been central to the development of training modules to support those using surveillance camera systems.
f. *Engagement with public and practitioners*. Perhaps most importantly, surveillance camera operators, law enforcement bodies and other practitioners singled out the value of proactive advice and wider engagement provided by the BSCC. This enabled surveillance operators to gain early advice, ensure standards were met and costly errors avoided. No such provision has been made to replace this important function. In this sense, regulation and oversight can be seen as a mechanism to *facilitate public safety initiatives*, rather than obstruct them. Additionally, the absence of such information may lead users to highly conservative interpretations of the law which may dissuade legitimate uses of surveillance technology for public safety.
g. *Proactively addressing issues of emerging concern*. Two illustrative examples include (i) the formalisation of governance structures regarding Automatic Number Plate Recognition cameras (a system that potentially operates the largest surveillance database in Europe); and (ii) addressing potential security risks brought by Chinese manufactured surveillance cameras in sensitive public sites.

The value of these activities, both statutory and non-statutory, are widely recognised across surveillance camera users, civil society organisations, industry professionals, academic experts, regulators and law enforcement communities. The BSCC has become a single point of contact for users, installers and the general public. No provision has been made to replace these activities in the provisions of the DPDI Bill as currently constituted. Any belief that such functions will happen automatically through the casework of stretched public bodies with notional oversight of this space appears unrealistic. As such, these activities will likely cease to exist.

Further analysis of the changes and additional oversight gaps.
The DPDI Bill fails to recognise the complexities of the current regulatory landscape and the protections offered by the BSCC in an era of increasingly intensive advanced and intrusive surveillance. Without a clear plan for how such activities and functions are replaced, abolishing the BSCC creates oversight gaps and will create, rather than remove, regulatory complexity. The following sections consider the above rationale for removing the BSCC role and outlines further implications for the oversight of surveillance cameras and biometric materials:

Duplicated oversight. The claim that surveillance camera oversight is duplicated appears to largely rely on three arguments: (a) that two codes of practice relating to surveillance cameras exist, (b) that data protection is the foundation for addressing potential surveillance harms, and (c) for all other matters, equivalent and sufficient oversight occurs in other public venues or through

alternative existing mechanisms. None of these arguments bear robust scrutiny. Moreover, using such arguments to shape legislation will generate further oversight gaps. This conclusion is further supported by the following:

> Regarding (a), surveillance operators, senior law enforcement representatives, academic experts, regulators, and the authors share similar views over the demonstrable differences between the ICO's 'Video Surveillance Guidance' and Government's SCCoP. The ICO 'code' is a non-statutory guidance document that relates to the processing of data captured and created by surveillance camera systems. The Government SCCoP is a statutory code *specifically covering all elements of public space camera systems* delivered by identifiable public agencies.
>
> On (b), significant differences exist difference between 'data protection' and 'surveillance'. The latter is not reducible to the former. This difference is widely accepted, understood, and agreed on by experts and practitioners in many advanced democratic societies legitimately using technology to protect the public. As such, stating such differences between data protection and surveillance is not controversial. Attempting to reduce surveillance into data protection limits recognition of potential surveillance-related harms, restricts prospects for their mitigation and denies opportunities for remedy. It constitutes a depletion of meaningful oversight.
>
> While overlap clearly exists between data protection and surveillance (such as in the use of data generated during the course of surveillance operations), the disparities are significant. Acknowledgement of this difference is precisely why other UK legislation aimed at regulating surveillance activities exists.
>
> Surveillance practices, particularly those pursued through advanced biometric technologies, engage a range of fundamental rights that extend beyond issues of data protection and privacy. These include the freedoms of assembly, association and expression. Relatedly, many surveillance activities implicate fundamental rights irrespective of matters concerning personal data. These include collective group-level, harms including profiling and categorisation and disparate technical performance across demographic groups. Such outcomes implicate the prohibition of discrimination.
>
> For (c), available material and justification for the DPDI Bill claims the existence of sufficient and comparable oversight mechanisms delivered by public bodies or other means. The main venue would be a reconstituted ICO, discussed above. Added to this, the ICO's own request for extra resources and capability challenges the argument that they already duplicates the work of the BSCC. Regarding other oversight venues, other than a superficial namechecking of these organisations, public documentation offers no detail on how such functions will be delivered. Many named bodies have either limited or no discernible track record of engaging with, or having influence over, the oversight of surveillance cameras or biometric materials. Confusion is also apparent in publicly stated Government reasoning over the difference between inspectorate roles, and oversight and regulatory functions. Added to this are questions over independence.

A 'principles-based approach' to oversight. Good reasons exist to limiting the specificity of technology-focused legislation, particularly when seeking to avoid any legislation becoming dated. Several issues arise over the way the DPDI Bill has been presented as a 'principles-based approach':

a. The Bill and its supporting documentation contain no detail on what these principles are and very little on how they will be enforced.

b. The Bill contains no mention of guidance or compliance mechanisms aside from those pertaining to data management. Key to the effectiveness of a principles-based approach is the relationship between law and policy. While law can set the overall direction in more abstract terms, clearly specified responsibilities, standards, guidance and policies are the means to implement such ambitions in a meaningful sense. This relationship was at the heart of the 2020 Court of Appeal judgment on the legality of facial recognition in *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058]*. Moreover, the same court made explicit mention of the very policy the Bill proposes to erase, the Government SCCoP, as one source of clarity in this regard (paragraph 109).
c. The Bill is not devoid of all specificity, however. Direct mention is made of the decades-old and (now) relatively uncontroversial biometric materials concerning DNA and fingerprints. The Bill makes no reference to practices that have since developed. This is significant because of its provision for the limited transfer of biometric oversight (on PACE s63G and National Security Determinations concerning the retention of biometric material) to the Investigatory Powers Commissioner. This transfer remains focused solely on these two biometric materials. It is surprising that a proposal which claims to be 'future proof' is so selective in its reference to biometrics. This approach also risks a de facto segregation in the oversight of different biometrics techniques.
d. Implications of emerging technologies: Among other developments in this field, significance public interest – and, according to peer-reviewed academic research, public concern – is focused on one such form of biometric surveillance: facial recognition technology. Other experts and public bodies have called for more detailed rules for uses of this technology. This point has added significance given current concern over declining levels public trust and confidence in the police and their importance for maintaining legitimacy. Reference to 'remote biometric identification' could be one entry point to addressing this issue.

Complementarity between the BSCC and other oversight bodies also risks complicating and weakening the wider regulatory ecosystem, affecting the bodies that remain after the Bill acquires assent.

Future considerations

The above sets out the roles, activities and functions that will be lost, and the gaps in oversight that will arise, with the abolition of the BSCC role. The following advances some considerations over future directions for maintaining and enhancing oversight in this area:

- It is essential that the SCCoP, along with a designated vehicle to ensure compliance, is retained.

- The Code and attendant compliance-related activities are heavily embedded into the work of surveillance camera operators and users. These tools are also popular among practitioners and are unequivocally seen as a means to raise standards.

- It is unrealistic to assume activities designed to maintain equivalent standards will emerge without a clear designation of responsibilities and resources is unrealistic.

- Rolling back oversight at a time of AI-driven surveillance tools, and during a period of highly polarised debate is likely to create additional challenges for surveillance users to gain trust, legitimacy and support within the communities they aspire to serve.

- A clear central code of practice, one that addresses the broader range of issues beyond data protection, provides certainty for surveillance operators and the public.

- The Bill intends to scrap Parliamentary reporting obligations covering the oversight of surveillance cameras and on the handling of biometric materials. Such annual public reporting mechanisms are essential to the maintenance of transparency and accountability, add meaning to often stated aspirations for 'surveillance by consent', promote trust and, hence, legitimacy, for public surveillance activities.

- Value clearly exists in exploring the retention of the BSCC role in some capacity and, in the authors' view, strengthening it to accommodate future oversight challenges.

- Surveillance is not reducible to data protection, particularly in an era of advanced-AI enabled tools. Should the BSCC role and associated functions be abolished, a next obvious venue for oversight is to explore how the Investigatory Powers Commissioner's Office (IPCO) may be well placed to adopt some of these functions.

INTRODUCTION AND CONTEXT

Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. These new and advancing technologies hold clear potential to enhance public safety, yet at the same time, have the capacity for significant individual and societal harm. Recent technological innovations have given surveillance cameras unparalleled capabilities to monitor and track the lives of people. Similarly, advances in new biometric identification technologies, such as facial recognition, behaviour monitoring and gait analysis, are increasingly integrated into the overt surveillance infrastructure. These technologies promise a range of perceived benefits, including enhanced public safety and more efficient access to services. However, the possibilities for integrated surveillance technology, driven by Artificial Intelligence (AI) and supported by the Internet, create genuine public anxiety over civic freedoms and human rights. The potential for intrusion and the impact on various rights brought by these advanced tools is arguably equivalent to many of the heavily regulated covert surveillance techniques and practices. Within this context, genuine, meaningful and trustworthy governance – to ensure the safe, responsible and legal use of surveillance tools – is urgent and pressing. The UK, in accordance with most advanced democracies, ensures that the responsible, legal and ethical use of public surveillance is addressed through forms of statutory independent oversight.

Concerns about the governance and oversight of technologically mediated state surveillance are particularly pressing given the pace of technological innovation and the speed with which it is deployed in public settings. For example, and as reported in May 2023, police use of one of the most heavily debated biometric surveillance techniques, Facial Recognition Technology (FRT), is set to accelerate. This is evidenced by the Minister of State for Crime, Policing and Fire's expressed desire to embed facial recognition technology in policing and is considering what the Government can do to facilitate this outcome.[1] This is likely to include the integration of this technology with police body-worn video despite concerns about its efficacy and levels of public support.[2] More recently, in August 2023 The Defence and Security Accelerator (DASA) fund was instructed by the Home Office to finance a 'Market Exploration' with the aim of enhancing the capability and feasibility for law enforcement and other security uses in the UK.[3] The Government has also announced plans to radically transform the scale and size of facial recognition reference databases beyond custody images to include passport photographs and images from the Police National Database.[4] In this context of accelerated deployment of advanced biometric surveillance tools, the consensus around elevating trust and confidence in the police, and in comparison to the more cautious approach adopted by many other advanced democracies, issues of meaningful oversight and regulation are of paramount concern.

It is widely accepted that current UK systems of oversight for public surveillance and biometric techniques are complex and would benefit from greater clarity. Many arguments exist in this space. The stated Government position is that overlap and duplication exists between different oversight bodies and that this creates difficulties for policing, local authorities and other public agencies seeking to enhance public safety (see below). These governance and oversight mechanisms are also difficult for the general public to interpret and understand. Others, including several civil society groups, have argued that current oversight is fragmented and insufficient, making it possible for potent new surveillance tools to 'fall through the gaps' and receive little regulatory scrutiny.

[1] See evidence to Public Bill Committee, https://bills.parliament.uk/publications/51173/documents/3425
[2] Interview with the Biometrics and Surveillance Camera Commisioner
[3] See funding call available from: https://www.gov.uk/government/publications/facial-recognition/market-exploration-document-facial-recognition
[4] https://www.theguardian.com/uk-news/2023/oct/02/uk-passport-images-database-could-be-used-to-catch-shoplifters?CMP=share_btn_tw. It is important to note that many images held on the Police National Database were judged by a 2012 High Court ruling to be held illegally [*RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] EWHC 1681 (Admin)*]. In October 2023 the Scottish Biometrics Commissioner described this latest plan as "egregious", "unethical and potentially unlawful" (https://www.biometricscommissioner.scot/news/commissioner-responds-to-statement-by-policing-minister-for-england-and-wales-about-uk-police-national-database-pnd/).

This report

This report considers changes to oversight mechanisms of overt surveillance camera and biometrics governance following changes proposed in the Data Protection and Digital Information (DPDI) Bill (no.2) (hereafter, "the Bill" or "DPDI Bill") presented to Parliament in 2023.[5] The primary focus are provisions in the Bill (specified in Part V) that relate to the Office of the Biometrics and Surveillance Camera Commissioner (OBSCC) as established under the Protection of Freedoms Act 2012. The report was commissioned by the OBSCC in January 2023. The report itself and the authors' analysis is wholly independent. The research process underpinning the report incorporates: a review of relevant literature, including consideration of other reports that have bearing on this subject; analysis of relevant provisions in this Bill and germane legislation; an overview of the roles and functions of the OBSCC; and interviews with leading experts, regulators and stakeholders holding insight and experience in the governance, oversight and use of surveillance and biometrics. The latter includes leading actors responsible for policing, regulation and service provision in this area. This report has therefore prioritised the perspectives of those operating public surveillance systems and engaged in uses of biometrics materials, and sought the views from those with national roles governing how such systems should be operated. Annex I lists those interviewed and consulted with. The report seeks to identify and analyse potential and likely ramifications of the provision of the Bill, with specific reference to identifying areas of biometric and surveillance camera oversight that will be lost once the BSCC role is abolished. Unless clearly attributed to others through quotes or other means, all expressed views belong to the authors.

An interim report offering summary findings (see Annex III), was presented to the Bill Committee by the BSCC in May 2023. Elements of these initial findings were discussed at the House of Commons Public Committee stage and recorded in official reporting during the same month.[6]

The report is structured into three main parts. Part One reviews provisions in the DPDI Bill relating to the oversight and governance of biometrics and surveillance and the role of the BSCC. Part Two reviews the statutory and non-statutory roles and functions of the BSCC. Part Three, analyses the implications of the Bill and gaps in surveillance oversight arising from the abolition of the BSCC role.

[5] Data Protection and Digital Information (DPDI) Bill (no.2) as introduced is available here: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf

[6] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf

PART ONE: THE DATA PROTECTION AND DIGITAL INFORMATION (NO.2) BILL

Section One of this report focuses on Part V of the Data Protection and Digital Information (DPDI) (no. 2) Bill ("the Bill" or "DPDI Bill") as it relates to existing functions of the Biometrics and Surveillance Camera Commissioner (BSCC). The Biometrics and Surveillance Commissioner role is a merger of two separate oversight roles (The Surveillance Camera Commissioner (SCC) and Biometrics Commissioner (BC)) established under the Protection of Freedoms (POFA) Act 2012.[7]

The original Bill was sponsored by The Department for Digital, Culture, Media and Sport (DCMS), while Nadine Dorries was serving Minister, before being withdrawn and reintroduced under the aegis of the newly constituted Department for Science, Innovation and Technology (DSIT). Part V of the of the Bill is sponsored by the Home Office. Where relevant to issues of biometric and surveillance camera oversight, aspects of the wider DCMS/DSIT sponsored elements of the Bill are discussed below.

The Bill followed a 2021 DCMS consultation exercise entitled "Data: A new direction" issued in September 2021.[8] Over 500 individuals and organisations provided responses, although to date none of these submissions have been published. The Government response to the consultation was last updated in June 2022. [9] The Government response acknowledges the range of views over the impact on surveillance oversight. However, is does not appear to engage with any of the expert critique offered during the consultation (often self-published by contributors) and it is difficult to discern the bearing of this debate on the shape of the Bill. The Bill was introduced to the House of Commons on 8 March 2023 and, at the time of writing (summer 2023), has progressed to Commons Report stage.

Provisions relevant to the Office of the Biometrics and Surveillance Camera Commissioner

Most relevant to the OBSCC, and to the oversight of surveillance and biometrics more generally, is the tabled removal of provisions contained in Chapter 1 of Part 2 of the POFA 2012. Among other changes, the effect of the Bill would be to remove the obligation on the Government to publish a Surveillance Camera Code of Practice (SCCoP) and to remove the post of the SCC whose functions are derivative from the SCCoP. Clause 104[10,11] of the Bill also proposes to amend section 20 of the POFA 2012 by abolishing the role of the BC with some limited casework functions transferred to the Investigatory Powers Commissioner (IPC) and others allowed to lapse (e.g. reporting functions). The Government-issued explanatory notes accompanying the Bill makes reference to the role of the Information Commissioner in "*continu[ing] to provide independent oversight of the use of biometrics by all bodies, including the police*".[12] Section Three of this report offers further detail on these and other proposed changes.

It should be noted that the Bill proposes substantial changes to the ways in which data processes will be regulated in the future, with significant structural and procedural changes to the existing data protection regulatory regime in the UK. Notably, the Information Commissioner's Office (ICO) will be replaced with a new 'Information Commission' with revised roles and functions.

[7] https://www.legislation.gov.uk/ukpga/2012/9/data.pdf
[8] Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf
[9] Available from https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#annex-b-list-of-organisations-that-responded-to-the-consultation
[10] Note: the numbering of some DPDI Bill clauses changed slightly following the Public Committee Stage in the house of Commons during May 2023. Because this report also draws on materials relating to the development of the Bill (e.g. government companion documents), and because the numbering may change again through the Bill's passage through Parliament, the original Clause numbers are retained. This is done with the assumption that the Bill as originally introduced will be easier to locate in the future. All altered clause numbers are footnoted with numbering current at the time of authoring this report (August 2023).
[11] Clause 111 in the version amended after Commons Public Bill Committee stage
[12] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265en.pdf

Any comparison between existing ICO functions and the new proposed Information Commission needs to take account of this. It is also important to note that, notwithstanding the above claim that 'continu[ed]… independent oversight of biometrics' (Ibid.), no specific detail is provided with regard to how, in the absence of a dedicated Biometrics Commissioner, the new Information Commission will provide oversight of biometric materials on matters that extend beyond data protection. This issue was highlighted in interviews with key stakeholders below.

Stated rationale for the removal of the BSCC role

The public position of the Government in support of Part V of the Bill focusses on, but is not limited to, themes around, simplification, duplication and a principles-based approach to regulation:

Simplification

It is widely accepted that existing oversight of complex surveillance practices is fragmented and requires simplification. Many recent reviews of and reports on biometric surveillance and digital policing[13] have highlighted the possibilities for confusion that may arise from the range of oversight mechanisms and regulation in this space. Agencies active in this area have different remits and varying degrees of formal regulatory authority. Overly confusing oversight regimes may not only complicate the provision of public safety, but may also denude regulation by allowing selective compliance. As such, a clear case has been made for streamlining oversight. In order to achieve simplification, provisions in the Bill propose to transfer selected biometrics oversight functions to the IPC and abolish those relating to surveillance cameras. Governance of the latter is assumed to be sufficiently covered by the new Information Commission and other existing agencies and processes. However, it has been argued by many expert-led reviews,[14] and stated in a relevant appellate court judgement,[15] such 'streamlining' needs to be companioned with clearly specified responsibilities, standards, guidance and policies, and that this is especially the case when transferring regulatory responsibilities between agencies.

The detail and merits of this argument are discussed throughout this report. To help navigate this issue, Annex II lists organisations regularly mentioned in discussions of surveillance oversight.

Belief in sufficient existing oversight coverage

The stated Government position relies on the argument that sufficient oversight currently exists for the governance of both public surveillance and of biometric tools. This position further relies on the assumption that the existing ICO, and presumably the new Information Commission, provides many of the oversight functions currently undertaken by the BSCC.[16] The following extract from the Bill's Explanatory Notes is an illustrative example of this approach:

> *"Clause 105[17] subsection (1) abolishes the office of Surveillance Camera Commissioner. Subsection (2) repeals Chapter 1 of Part 2 of POFA, repealing the requirement for a Surveillance Camera Code and related provisions. This removes duplication in oversight of overt surveillance (for example CCTV systems) used by the police and local authorities. The Information Commissioner already has oversight of the use of*

[13] e.g. Ada Lovelace Institute (2022) *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, P71-72 available from https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf; House of Lords Justice and Home Affairs Committee (2022) *Technology Rules: The advent of new technologies in the justice system*, https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf; AI NOW (2021) Regulating Biometrics: Global Approaches and Open Questions, New York City: AI NOW (esp. chapter 6) https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions; ICO (2019) ICO investigation into how the police use facial recognition technology in public places https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

[14] Ada Lovelace Institute (2022), House of Lords Justice and Home Affairs Committee (2022)

[15] *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058].*

[16] Where suitable and best aligned to the subject of discussion this report refers to oversight roles and responsibilities with reference to the postholder, rather than the office they represent (for example, the 'Biometrics and Surveillance Camera Commissioner', rather than 'Office of the Biometrics and Surveillance Camera Commissioner').This is because it is the Commissioner, rather than the office that holds legal personality, hence 'Commissioners' are referred to throughout where possible and relevant.

[17] Clause 111 in the version amended after Commons Public Bill Committee stage

> *personal data under the Data Protection Act 2018, including data captured via surveillance camera systems, by all controllers, including the police and local authorities. The Information Commissioner's Office has also published guidance on the use of such systems. This means that the Information Commissioner will continue to provide independent oversight and regulation of this area, without duplication by the Surveillance Camera Code and Commissioner, making it easier for the police, local authorities and the public to understand and comply with any requirements."*[18]

This claim of duplicated oversight relies on the argument that two codes of practice relating to surveillance cameras exist. On a cursory reading, they appear to cover similar ground given both apply to public space surveillance camera systems. Overlaps and differences between the ICO and Government codes are discussed in detail in Part Three of this report, as are the perspectives of senior law enforcement and local authority practitioners concerning this perceived duplication. For the purposes of elaborating one essential difference between the codes, the ICO code is a non-statutory guidance document that relates to *the processing of data* captured and created by surveillance camera systems. The Government SCCoP is a statutory code specifically covering *all elements of public space camera systems* delivered by identifiable public agencies. Of further note is the sequence with which the Information Commissioner and Surveillance Camera Commissioner roles were established. The ICO was established in statute 28 years earlier than the SCC role. The existence of such duplication between the two roles would raise significant questions over why it was deemed necessary to establish the latter under the POFA 2012.

Similarly, and with regard to the biometrics-focused elements of the BSSC role, the Government also considers police uses of biometric data in non-terrorism related cases to be sufficiently covered by the ICO:[19]

> *"Subsection (4)(d) [of Clause 104][20] removes the function to review the retention and use, by the police and others, of fingerprints and DNA profiles not subject to a National Security Determination, whether this biometric material has been taken and retained under PACE, the Terrorism Act 2000, the Counter-Terrorism Act 2008, or the Terrorism Prevention and Investigation Measures Act 2011. This removes duplication in oversight, as the Information Commissioner has a duty to keep under review the use and retention of personal data by all controllers, including the police".*[21]

A further strand of this argument is the Government view that data protection provisions provide sufficient coverage for police uses of biometric tools and for wider uses of overt public surveillance cameras:

> *"Under the DPA 2018, the Information Commissioner provides independent oversight of all [data] controllers' use of all personal data. This includes the use of biometrics and surveillance cameras… The Information Commissioner has extensive regulatory powers and issues its own guidance to controllers including the police, which is published… This Bill would simplify the oversight framework for the police use of biometrics and police and local authority use of surveillance cameras. It would abolish the Biometrics and Surveillance Camera Commissioners' posts, and the Surveillance Camera Code. The Information Commissioner's Office, which covers the use of all personal data by all bodies, remains in place".*[22]

Beyond the ICO, the Government also cites other organs as providing oversight in this space. This includes the Equality and Human Rights Commission[23] and the Home Office Forensic Information Database (FINDS) Board (formerly called the National DNA Database Strategy

[18] UK Government's DPDI Bill Explanatory notes, p.89 https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265en.pdf
[19] Notwithstanding the transference of PACE s.63G casework to the Investigatory Powers Commissioner (see below).
[20] Clause 111 in the version amended after Commons Public Bill Committee stage.
[21] UK Government's DPDI Bill Explanatory notes, p.88
[22] UK Government's DPDI Explanatory Notes, p.88
[23] House of Commons Official Report of the Public Bill Committee Debate p.273 https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf

Board). The Government considers the FINDS Board as holding "*similar oversight of the police national fingerprint database*" to the Biometrics Commissioner and offering "*the Secretary of State with a power by affirmative regulations to amend the scope of this Board*". [24]

The BSCC role focuses on the oversight of public bodies, primarily policing agencies and local authorities. Data protection regulation, overseen by Information Commissioner, covers both public and private entities. Housing oversight in the latter may therefore provide wider scope and address complexities of regulating public-private surveillance activities. This is a relevant point given the increasing integration of publicly and privately owned surveillance camera systems and because many private systems operate in 'public' places. In addition, the Information Commissioner holds a UK-wide remit, whereas the BSCC's geographic remit is primarily England and Wales, although there is a biometrics function relating to national security that extends beyond this to Scotland and Northern Ireland. Whilst giving responsibility for surveillance oversight to a data protection focused Information Commission may offer greater coverage over the UK's devolved administrations, potential also exists for this to further complicate the regulatory landscape. For example, Scotland has a dedicated Biometrics Commissioner, which is a Holyrood Parliamentary appointment whose statutory obligations reference other relevant legislation, including the POFA 2012 and the activities of the BSCC, and as such creates governance complexity in the pursuit of simplicity. Implications connected to devolution are discussed in more detail below.

It is important to note that the Information Commissioner and BSCC offer different forms of oversight. For example, only the ICO can properly be considered as a regulator given the absence of investigatory, punitive and regulatory powers afforded to the BSCC. Accordingly, an argument can be made that 'ICO-type'[25] regulation of public surveillance brings additional weight through the option of formal sanction. However, such arguments are tempered by the Information Commissioner's stated position of not fining public bodies that breach data protection laws, and the history of limited investigations into surveillance-related issues, especially in the realm of public space surveillance camera systems (see Part Three). It is also important to note, that the Information Commissioner is principally concerned with the protection of the rights of data subjects, while the BSCC is more broadly concerned with keeping strategic policies and practices of relevant bodies (notably the police) under review and reporting annually to Parliament.

This discussion is further complicated by the claim that ICO surveillance oversight is duplicated by the BSCC. Part of this complexity arises from the lack of detail around future oversight arrangements for surveillance and biometrics. The ICO have been receptive to the idea that existing data protection principles and legislation can satisfactorily cover the regulation of public space surveillance camera systems. They have also clearly stated previously that this "expansion of our regulatory remit" is "subject to appropriate funding" and that they "await further detail on how any transfer of functions would work in practice".[26] The emphasis on additional resourcing would imply the sense that, rather than erasing a redundant and duplicated form of oversight, the perspective of the key regulator is that delivering BSCC functions is not a sense of 'business as usual' but would necessitate an expansion of their role. Indeed, the ICO consultation response to the original plans for abolishing the BSCC role explicitly stated that any such additional functions would be "*subject to appropriate funding being available*".[27]

Added to this, given the latest data breaches involving PSNI, Norfolk/Suffolk and Cumbria

[24] UK Government's DPDI Bill Explanatory notes, p.13.
[25] A relevant, albeit technical, detail applies here. The Bill does not strictly propose that the Information Commission takes over OBSCC functions because Clause 107 of the Bill proposes the abolition of the Information Commissioner and replacement with an 'Information Commission'. However, given the ICO has existed for 37 years and holds unparalleled institutional expertise and memory in the regulation of data protection law, it seems unlikely an entirely new and separate organisation comprising an untapped comparable level of expertise will emerge.
[26] ICO (2021) 'Response to DCMS consultation "Data: a new direction"', p.88 available fromhttps://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[27]ICO (2021) 'Response to DCMS Consultation', P.24.

police forces it is reasonable to assume the reconstituted ICO would require larger resources to ensure public confidence around their existing areas of practice even before public space surveillance issues are brought into consideration.

The ICO is a larger and better resourced entity than the OBSCC. The ICO strategic plan - ICO25[28] - sets out their strategic direction across a wide range of areas. Notable here, is that the plan contains just a single reference to "CCTV", no reference to public space surveillance, and mentions of biometrics are sparse and largely focused on working with industry. One argument could be that the breadth of the ICO strategy, and their remit, could lend adaptability of oversight activities. A counter argument is that the BSCC also incorporates the capacity to adapt and address emerging issues of importance.

At this stage, it is also important to recognise how much of the language around the future 'transfer' and 'delivery' of BSCC activities is vague and indeterminate. Detail on how the BSCC's wider functions would be addressed are limited. No detail is offered on how this would work in practice. As it currently stands, the provisions in the Bill simply abolishes the functions of the BSCC relating to public space surveillance cameras, and transfer biometrics casework functions to IPCO. This implies that there is an assumption that oversight functionalism will be covered to a satisfactory level by the new Information Commission and other relevant agencies. The request for extra resources and capability by the ICO challenges the argument that the BSCC duplicates the work of the ICO.

A 'principles based' approach

Government documentation also points to the intention of adopting a 'principles-based approach' to address the problem of highly specified technology-focused or otherwise piecemeal approach to legislation which can become quickly outdated. Moreover, detailing specific surveillance tools may allow new technologies to escape regulatory scrutiny by virtue of not being specified in the legislation. The extent to which individual techniques and technologies are specified in legislation is a subject of wider debate, with valid arguments on both sides. The central premise is reasonable and reflects an ongoing concern reflected in the academic literature and other analysis of this topic.

While little elaboration of the principles-based approach is apparent in the Bill text, a signal of Government thinking around this is discernable from commentary on parallel issues. This includes the Government response[29] to (and rejection of) recommendations issued by the House of Lords Justice and Home Affairs Committee review of digital policing:

> *"For policing specifically, there are already many safeguards. The data protection, equalities and human rights framework set by parliament has created a principles-based framework. Together with the foundational Peelian principles for policing, now enshrined in the Standards of Professional Behaviour (schedule 2 of the conduct regulations), the existing legal framework requires the safe and ethical deployment of new technologies. Therefore, the Government will focus on encouraging policing in particular, (sic) to provide innovative solutions which identify and promote best practice…The UK is a signatory to the OECD Principles. Internationally the Government works with like-minded countries to support the responsible use of AI. The Government's Plan for Digital Regulation notes the importance of exploring a range of outcomes-focused regulatory and non-regulatory tools to promote a pro-innovation approach".* [30]

Prominent here are the data protection and equalities and human rights frameworks overseen by the ICO and EHRC respectively. Additional reference is made to nine (broadly conceived)

[28] ICO (2022) *ICO25 – empowering you through information*, https://ico.org.uk/media/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan-0-0.pdf
[29] https://committees.parliament.uk/publications/22773/documents/167387/default/
[30] House of Lords Justice and Home Affairs Committee (2022) *Technology Rules: The advent of new technologies in the justice system*, https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf

'Peelian Principles' developed around the time the Metropolitan Police was established in 1829,[31] as a mechanism ensuring ethical uses of digital technology in policing. Also relevant is the invocation of international standards and contexts, particularly given possible divergence in the UK approach compared to that pursued by other countries, notably among EU nation states.[32]

Such belief in police self-regulation appears harder to justify in the context of ongoing public and political debates surrounding police accountability. It also misunderstands the crucial differences between inspection and regulation and the consequences this has for upholding human rights. For example, Baroness Casey's recent independent review into the standards of behaviour and internal culture of the Metropolitan Police Service is clear on limits to the enactment of Peelian principles in policing, citing 'optimism bias' and 'a tick box approach to critical reports',[33]adding that 'structures of governance and scrutiny are relatively weak'.[34] Such observations also resonate with approach observed by independent scrutiny of policing uses of surveillance technology, where seemingly relevant statutes, regulatory instruments and oversight processes are listed without any detail of how they would be operationalised or otherwise apply.[35] This may in part be attributed to the recognised complexity of the regulatory landscape, and the difficulties this generates for policing, but also points to the limits of self-regulation in this space. This point is also relevant to the only UK legal proceedings addressing facial recognition technology, the appellate court expressed concern over the excessive discretion police policy frameworks afforded to officers in the deployment of FRT. The Court found that the policy frameworks established by the police were inadequate, and could not be considered 'in accordance with the law'.[36]

The value of the principles-based approach as a means to accommodate future developments in surveillance and biometrics innovation is often advanced as a means to facilitate adaptability is often expressed as a justification.[37] This deliberate lack of specificity as a means to provide oversight of future tools is discernible in the suggested expansion of existing mechanisms. For example, in the Bill Explanatory Notes reference is made to an intended future role of the FINDS board, an entity originally established to support the oversight of DNA data:

> *"Clause 105[38] also introduces a new power for the Secretary of State to change the databases the FIND-SB oversees by adding or removing a biometric database used for policing purposes. The regulations to enable this will be made under the affirmative procedure. This power is intended to enable flexibility in the board's remit given the pace of technological change in this area and the need for clear and consistent oversight. To support policing to meet the requirements of the DPA and PACE, the FIND-SB will produce codes of practice on the destruction of biometric material and erasure of this data from a database".*[39]

Key to the effectiveness of a principles-based approach is the relationship between law and policy. While law can set the overall direction in more abstract terms, policies are the means to implement such ambitions in a meaningful sense. Moreover, such policies are easier to refine and

---

[31] See *inter alia* Benyon, J. (ed.) (1984) Scarman and After: Essays Reflecting on Lord Scarman's Report, the Riots, and Their Aftermath, Oxford: Pergamon Press

[32] See, for example, the May 2023 EU Parliamentary vote to ban uses of FRT in public spaces (with notable exceptions).

[33] Baroness Casey Review (2023) Final Report: An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service, available from https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023a.pdf p.14.

[34] Casey Review (2023) p.18

[35] Fussey and Murray (2019) *Independent Report on the London Metropolitan Police Trial of Live Facial Recognition Technology*, University of Essex Human Rights Centre https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf . Also relevant here is the Court of Appeal judgment in *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058]* concerning the excessive discretion afforded to officers in the deployment of facial recognition technology.

[36] *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058].*

[37] Although it is also important to flag that the EU AI Act (draft) text contains a list of 'high risk' technologies, which it can be amended relatively straightforwardly.

[38] This became Clause 106 in the Bill (no.2) form as introduced and then Clause 113 in the version amended after Commons Public Bill Committee stage.

[39] UK Government's DPDI Bill Explanatory notes, p.90

amend and, as such, are more agile and capable of accommodating developments in this space. Indeed, this relationship was at the heart of the 2020 Court of Appeal judgment on the legality of facial recognition in *R (on the application of Bridges) v Chief Constable of South Wales Police.*[40]

The role of more precise policies is also critical when considering the different types and emerging uses of information elicited by biometric techniques. As the 2022 Ryder Review's independent legal analysis of biometric data governance sets out, levels of intrusion brought by the *classification* of biometric data, which underpins profiling activities and is less regulated, is paralleling the more regulated practice of biometric *identification*. Enforceable policies and codes of practice gain particular value in targeting regulation and giving shape to a meaningful and enforceable oversight regime:

> *"future regulation of biometric data should embed equal safeguards for biometric categorisation systems as biometric identification systems… It is not possible to set out in the abstract, what the content of any of the envisaged codes of practice should be. However, they should impose clear, accessible, and meaningful standards against which deployments of biometric technologies can be assessed and reviewed… Provided there is clarity as to who has responsibility for issuing relevant codes of practice within a new legal framework for the regulation of biometric data… such codes should have a similar status for relevant stakeholders as the Code of Practice under the Scottish Biometrics Commissioner Act 2020. Relevant stakeholders should be required to comply to an applicable code of… A failure to comply with an applicable provision by a public authority would potentially be a public law error which could ground judicial review proceedings".*[41]

Underscoring the argument that such policies have agility, is the latest (2021) iteration of the SCCoP laid before Parliament by the Home Secretary under her legal obligation under the POFA 2012.[42] This governmental code addresses recent innovations in biometric surveillance and suggests approaches towards the governance of such technologies. Notwithstanding limits to its enforceability, and the Government argument that it duplicates ICO guidance, this Code goes beyond data processes, has a different function, is published as part of the applicable law by the Government, and is widely regarded by surveillance camera users as an essential tool for maintaining standards in the profession.

Transferring selected functions to other oversight bodies

Despite the stated aspirations for an approach that emphasises principles over specific surveillance activities and biometrics material, the Bill explicitly outlines provision for some specific biometric oversight casework: that involving fingerprints and DNA. One likely explanation for this is that these two techniques are plainly stated in the sections of POFA, the Bill proposes to replace. Mention of specific biometrics techniques in POFA occurred because the legislation was in part a response to a European Court of Human Rights ruling against the UK on the retention of Fingerprints, cellular samples, and DNA profiles.[43] The implications of naming and designating oversight for some forms of biometric material while leaving others unmentioned is explored in Part Three of this report.

The Bill thus proposes to transfer specific statutory responsibilities regarding biometric casework to the Investigatory Powers Commissioner. Specifically, the Bill makes provision for the transfer of the BSCCs judicial functions covering Police and Criminal Evidence Act (PACE) 1984 s63G provisions and National Security Determinations (NSD) casework covering the oversight and review of biometric data retention. The Bill makes no other requirement on the IPC for

---

[40] *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058].*
[41] Ada Lovelace Institute (2022) *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, P71-72 available from https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf
[42] Available from https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf
[43] *S and Marper v United Kingdom* 30562/04 [2008] ECHR 1581

biometrics oversight.

Overall, the stated position of the Government in relation to the roles and functions of the BSCC is that provisions within the Bill will simplify oversight; remove duplication; offer a sufficient principles-based approach to regulation and oversight; facilitate transfer of selected quasi-judicial functions of the BSCC to the IPC; that other necessary oversight activities are already covered by a blend of existing and newly reformed agencies; and that abolishing the BSCC role will not be to the detriment of policing or society. We argue that this approach generates significant gaps in the formal oversight of biometrics and surveillance practices in additional to erasing many positive developments aimed at raising standards and constructive engagement with technology developers, surveillance users and the public. We also argue that the new proposals fail to recognise: the complexities of the current regulatory landscape, the protections offered by the BSCC in an era of increasingly intensive advanced and intrusive surveillance, and that the abolishment of the BSCC leaves oversight gaps whilst at the same time creating additional regulatory complexity.

PART TWO. THE ROLE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

The Biometrics and Surveillance Camera Commissioner (BSCC) plays a vital role in the governance of the use of biometric materials and surveillance camera technologies by state and public service agencies. The key roles of the Commissioner are defined in legislation and include statutory and non-statutory activities. Combined these activities provide: important safeguards for users and citizens in a world where fast moving technologies offer the potential for individual and societal harm; guidance for those public agencies wishing to deploy these technologies; and, mechanisms to hold users of these technologies to democratic account. As such, the Commissioner and the Office, are a significant part of the oversight and stewardship landscape ensuring these technologies are used in the 'public interest'.

Calls for clearer oversight of public surveillance cameras arose through the early 2000s. A second phase of government capital finding for local authorities' implementation of surveillance camera schemes concluded in 2001 had stimulated a rapid adoption and expansion of the technology.[44] Slightly later in the decade (2008) the European Court of Human Rights ruled against the UK over police retention of fingerprint and DNA profiles of those arrested yet not convicted of any offence. The unanimous Strasbourg judgement, *S & Marper V UK*, ruled that such practices contravened Article 8 of the European Convention on Human Rights, the right to respect for private and family life.[45] This ruling influenced the development of the UK Protection of Freedoms Act (POFA) 2012 which established a designated "*Commissioner for the Retention and Use of Biometric Material*" (henceforth the "Biometrics Commissioner") and set out judicial functions required to oversee the retention of fingerprint and DNA data.[46]

Initially, POFA created two Commissioners, the Biometrics Commissioner (BC) and the Surveillance Camera Commissioner (SCC). It is also important to note that POFA created the Surveillance Camera Commissioner role despite the prior existence of the ICO and their code of practice for CCTV. This suggests recognition at that time that data protection regulation was insufficient to providing effective oversight of rapidly developing surveillance technology. The two separate Commissioner roles were combined into one entity, the BSCC, in 2021. While it is difficult to locate public explanation for this merger, it would be reasonable to assume some tacit recognition of the overlapping concerns between the two Commissioner roles, for example due to the expansion of biometric surveillance technologies such as facial recognition. The Commissioner derives legal authority from POFA and, while wholly independent, reports directly to Parliament via the Home Secretary, and whose office is supported financially by the Home Office.

Surveillance Camera Oversight: Statutory Functions

The oversight of public space surveillance cameras is realised through statutory functions laid out in POFA and realised through the BSCC. Regarding the SCC functions, the legislative requirements of the Commissioner are principally related to the Government's Surveillance Camera Code of Practice (SCCoP). With respect to this section 34 POFA places responsibility on the Commissioner to *"(a) encourag[e] compliance with the [Government] surveillance camera code, (b) revie[w] the operation of the code, and (c) provid[e] advice about the code (including changes to it or breaches of it)*".[47] The

[44] Webster, C.W.R. (2004) The diffusion, regulation and governance of closed-circuit television in the UK. *Surveillance and Society*, Vol.2, No.2/3, pp.230-250.
[45] In a point solely of historical curiosity, the complainants 'S' and 'Marper', applied for judicial review over the police retention of their biometric data and the refusal of the latter to reconsider. The Administrative Court refused this application in March 2002 [[2002] EWHC 478 (Admin)]. This refusal was, eventually, overturned by the European Court of Human Rights, leading to the '*S & Marper*' ruling. One of the Administrative Court judges that refused this initial application in 2002 was Sir Brian Leveson. If the DPDI Bill passes in current form, Sir Brian Leverson, now the Investigatory Powers Commissioner, will hold responsibility for decisions over the retention of fingerprint and DNA material.
[46] S.20 of POFA.
[47] S.34 of POFA https://www.legislation.gov.uk/ukpga/2012/9/enacted/data.pdf

Commissioner also has a duty to report annually to Parliament on progress and activity relating to deployment and use of cameras and adherence to the SCCoP. The SCCoP is expected to cover all aspects of a public space surveillance camera systems, including purpose, procurement, technical specifications and deployment. The POFA legislation names those public agencies ('relevant authorities') which are expected to comply with the SCCoP: primary police forces, local authorities and other specified agencies (see below). The SCC remit covers the use of a range of different types of overt cameras, including static and mobile cameras, drones, ANPR and body-worn video cameras. The key purpose behind the legislation is to drive up standards, to ensure 'best practice' and to provide reassurance to the public that the cameras are being used appropriately and within the law.

The SCCoP, as laid before Parliament, is a unique document covering all aspects of a public space surveillance camera system. As a 'code' it is not legally enforceable. However, POFA states that "*relevant authorities must have regard to the surveillance camera code when exercising any functions to which the code relates*". Failure to act in accordance with the Code does not bring criminal or civil liability but may be admissible in relevant legal proceedings. As Section 33(4) of POFA states,

> *"A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings."*

The Code also sets out very clearly, how a designated agency should conceive of a system, how it should be designed, constructed and implemented, including all technical and governance matters. This includes compliance with all relevant legislation and how to approach new technological developments, including AI-driven systems such as FRT. It is in this regard that successive SCCs have interpreted 'public surveillance' broadly. For example, S.29(6) of POFA defines 'surveillance camera systems' reasonably broadly. While specifically naming CCTV and ANPR, POFA also widens the definition to technologies capable of capturing:

> *"(b)… systems for recording or viewing visual images for surveillance purposes, (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by [visual surveillance] systems"*[48]

This offers latitude for visual surveillance tools such as FRT and drones to be considered under the SCC remit.

Underpinning the 'purpose' of the SCCoP is the belief that agencies using such systems should comply with legislation and 'best practice'. Adhering to the Code provides these agencies with confidence and certainty regarding how they conduct public surveillance and offers public reassurance over appropriate use. An important point to note, is that the SCCoP covers all aspects of a surveillance camera system and is not confined to technical requirements or data processes. The DPDI Bill proposes the abolition of all SCC-related functions and, hence, this Code.

Tony Gleason, Chairman of Public CCTV Managers Association stated for this report,

> *"The Surveillance Camera Commissioner's Office are the experts in the field of public surveillance, the Code of Practice [the SCCoP] and associated technical specifications, together they provide the structure and guidance to give local authorities the confidence to deliver an effective system."*

A senior local government officer further argued,

[48] S.29(6)b & c of POFA

> *"The Code of Practice [the SCCoP] is an essential tool for guiding you through all elements of using a CCTV system, from considering whether the circumstances are right for installing a system, why the system should be installed, whether it is effective use of public funds and the technical standards required to make the system work – the Code has proven to be a really useful checklist of core issues for Councils to work through".*

Surveillance Camera Oversight: Non-Statutory Functions

To deliver the statutory functions set out above, SCC's have pursued a number of activities designed to ensure that the SCCoP delivers its purpose and to make sure that those operating such systems have clear guidance about how they should be used. Whilst many of these activities are not statutory, in that they are not directly specified in POFA, they are crucial in supporting the work of the Commissioner and without these activities the SCCoP could not be realised and oversight not achieved. These activities include the following:

National Surveillance Camera Strategy for England and Wales

The National Surveillance Camera Strategy for England and Wales (the 'National Strategy')[49] is closely intertwined with the SCCoP. The SCCoP sets out 'best practice' and expectations for those using surveillance cameras, whilst the National Strategy provides a mechanism for achieving them, including the relevant actions required to deliver the specifications of the Code. The National Strategy specifies several 'Strands' of activity, each led by an industry or appropriate expert.[50] In this respect, the National Strategy and the SCCoP emerges from a process of co-creation involving critical stakeholders and the Commissioner, which provides legitimacy and support. A further component of the Strand Lead arrangement is that it brings additional stakeholders into, and diversifies voices of, oversight of public surveillance. Further and related Commissioner-initiated practitioner engagement initiatives include the establishment of a Stakeholder's Forum and Advisory Board.[51] Along with the Code of Practice and the role of the BSCC itself, this National Strategy for raising technical and accountability standards among surveillance camera operators will also be erased with the passing of the DPDI Bill.

Tony Gleason, Chairman of Public CCTV Managers Association stated in an interview for this report,

> *"The 12 guiding principles set out in the Code of Practice and reflected in the National Strategy force users to ask themselves why are they conducting surveillance in the first place, what checks and balances need to be brought into play, and how to remain compliant with the law, including POFA and the DPA. They also add considerable value by raising issues like training and proper maintenance regimes, as well as making sure there is a pressing need for community consultation, and in doing there is an added layer of transparency and accountability."*

The Certification Scheme and Self-Assessment Tool

A key component of the SCCoP and the National Strategy has been the creation of a 'Certification Scheme', whereby camera operators demonstrating compliance with the SCCoP are certified by the Commissioner via a Self-Assessment tool.[52] This 'award' is a recognition of 'best practice' in the principles and use supporting a specific system and is designed to provide

[49] National Surveillance camera Strategy for England and Wales, URL: https://www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales

[50] The authors of this report have collectively served for over a decade in two such strand lead roles (Prof Fussey as Human Rights and Ethics Strand Lead, and Prof Webster as Public Engagement Strand Lead). As such, they hold detailed understanding of the application and impact of the National Strategy.

[51] A value for money argument also exists here given the BSCC role draws resource and expertise from a range of stakeholders in this manner. Another component of this is the more lateral integration of local authority practice and increased dialogue between law enforcement and local authority surveillance camera managers through the mechanisms outlined in this part of the report.

[52] BSCC Self-Assessment Tool, URL: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

assurances that these systems are used correctly. Interviews with surveillance camera managers revealed overwhelming support for the Certification Scheme, both in terms of guiding their own practice and in allowing them to provide reassurance in response to public concerns. Whilst the SCCoP applies to those public agencies specified in POFA legislation, not all have been certified or adhere to the requirements of the Code. Whilst the Certification Scheme is targeted at those public agencies, as specified in legislation (compulsory adopters), it is also open to voluntary adopters. These are agencies or companies that choose to apply for certification because they recognise the importance of being seen to used surveillance cameras proportionally and appropriately. Voluntary adopters include private companies like Marks and Spencer, universities, and local authorities operating outside the geographical jurisdictional boundaries of the Commissioner.

Tony Gleason, Chairman of Public CCTV Managers Association stated,

> *"The certification scheme has been brilliant, it sets a minimum standard, which everyone can adhere to. So, if my system, or any of our members systems are brought into question, then we can point to the certification scheme to say that we are abiding by the legal requirements of POFA – this should give everyone confidence about the use of systems."*

Alex Carmichael, Chief Executive Security Systems and Alarms Inspection Board (SSAIB) adds,

> *"The beauty of the Code [the SCCoP] is that it brings everything together in one place – operational requirements, the purpose of systems, guidance, training, procurement – globally it is the gold standard."*

Surveillance Camera Standards Group

The Surveillance Camera Standards Group[53] has been established within the framework of the National Strategy to define minimum technical specifications and standards necessary in a for surveillance camera systems that develop in sophistication and technical ability. These technical specifications relate to camera capability, image quality, data transfer, interoperability and storage capacity. The intention of these specifications is to inform manufacturers, suppliers, installers and users about the technical requirements of camera systems. This is particularly important for reaching evidential standards in criminal justice proceedings. Moreover, the lack of standardised technical specifications prior to the SCCoP resulted in variable image quality and formatting standards of image data used for investigations and prosecutions. This role of the BSCC has been credited with 'driving up standards' across the surveillance camera industry.

Tony Gleason, Chairman of Public CCTV Managers Association offered the following perspective,

> "*The Surveillance Camera Commissioner has been the focal point for designing a set of standards, and in guidance on how to reach those standards. Without his Office, technical standards would vary from one authority to another and the provision of systems would be fragmented and incompatible."*

A senior local government representative added,

> *"The Code [the SCCoP] has been an essential short-cut to identify the technical specifications required to confidently deliver a CCTV system…without this there is a risk that Council's will struggle to navigate their way through this complex environment, with a further risk that they will be at the mercy of commercial suppliers who will claim their products meet national requirements, when they don't. A national uniform standard has been invaluable to local authorities".*

[53] Surveillance Camera Standards Group, URL: https://www.gov.uk/government/publications/surveillance-camera-standards-group-terms-of-reference

The Buyer's Toolkit

A component of the National Strategy has been the development of a 'buyers toolkit' for users and installers. This guide sets out detailed procurement guidelines[54] for those responsible for purchasing and installing surveillance camera equipment and systems. This is intended to provide guidance and support so that future systems are of the right standard and purchased from reliable suppliers. Tim Raynor, Vice chair for the Video Surveillance Section, British Security Industry Association (BSIA) argued that "*the security industry is becoming ever more complex, both in terms of cybersecurity and ethical concerns, and there is a lot more to making a procurement decision than simply how much does it cost.*"[55] Following this guidance ensures buyers and installers arrive at informed decisions about whether surveillance can be justified as a solution to problems, and if deploying surveillance cameras is necessary. The toolkit offers advice on how to get the best out of prospective suppliers. It also allows security industry suppliers to demonstrate to their customers that they understand, and follow, good practice and legal obligations.

Tim Raynor, Vice chair for the Video Surveillance Section of the British Security Industry Association offered the following perspective on the Buyer's Toolkit,

> *"The Surveillance Camera Commissioner has been instrumental in producing a 'buyer's guide', written in plain English, so that someone responsible for procuring CCTV systems knows what they are doing. This has been critical in driving up standards. The next stage was to update this guide to bring in more advanced technologies, like FRT and AI. However, with the Commissioner's role being discontinued, this work will not 'sit' with anyone and won't be undertaken. This will be a big loss as there is nothing else out there covering this ground"*
>
> *The buyer's guide was a dynamic document, it worked well because it was a standard template that could be used as part of a procurement exercise and provided buyers with a sequence of questions and issues to be considered."*[56]

Training

Alongside the technical specifications established by the Surveillance Camera Standards Group has been the development of training modules to support those using surveillance camera systems. This includes the creation of service level agreements and compliance with all relevant legislation. Training includes guidance for operators, those managing systems and supervising operators, as well as training for those managing and sharing personal data.

Tony Gleason, Chairman of Public CCTV Managers Association highlighted the importance of this training role, and how it would be lost with the abolition of the BSCC role,

> *"Training is a really good example of why the role of the Surveillance Camera Commissioner is so important. POFA and the DPA say very little about training, but the Surveillance Camera Commissioner and the Code of Practice [the SCCoP] provide explicit guidance about training and the need for training to ensure equality and proportionality are realised, and to minimise the risks associated with discrimination and targeted surveillance."*

Interfacing with practitioners: further initiatives

The roles outlined above represent formal mechanisms to engage with developers, users and managers of public surveillance camera systems. Surveillance camera users and managers interviewed for this report were unanimous in their praise of the SCC role. The ability to contact the Commissioner and the responsiveness of the Commissioner and OBSCC staff was

[54] Surveillance Camera Commissioner's Buyers Toolkit, URL: https://www.gov.uk/government/publications/surveillance-camera-commissioners-buyers-toolkit
[55] Tim Raynor interview for this report.
[56] Tim Raynor interview for this report.

particularly commended. It can be further argued, that this availability of expertise and guidance embeds a measure of agility and adaptability into the use, management and governance of surveillance camera systems that will be lost once the BSCC is abolished. Such informal knowledge brokering and the facility to check aspects of regulatory compliance in a constructive, rapid and responsive way was seen as an important resource with multiple benefits. This included avoidance of costly mistakes that could incur financial and reputational damage to repair later and, crucially, mean their role in delivering public safety was more straightforward and, crucially, more effective. In this respect, regulation and oversight can be seen as a mechanism to *facilitate public safety initiatives*, rather than obstruct them. Police and other surveillance camera users' support for the value of such engagement is discussed further in Part Three of this report.

Less commented on yet also notable are the accounts of the current BSCC[57] and former BC highlighting how Parliamentarians regularly seek advice from postholders. As a former BC stated in his (unpublished) response to the initial DCMS consultation,[58]

> *"The importance of these functions has been recognised by Parliament and its Select Committee and by ministers. I was regularly asked by parliamentarians and select committees of both houses for my views on matters relating to the police use of biometrics or the use of biometrics in general and also whether ministers had discussed matters with me when any change relating to the police use of biometrics was being discussed. The late (and very sadly missed) Minister for National Security consulted me at some length when temporary changes were made in the granting of National Security Determinations in the Coronavirus Act. I reported on the fact of these conversations and laid out my view on the matter for MPs before they considered both the passage of the Act and its subsequent renewal and also made these publicly available."*

Interfacing with the public: Consent, legitimacy and accountability

A key element of the National Strategy is to engage stakeholders and the general public to build awareness about the use of surveillance cameras in society. This has several implications. First, public awareness is critical to supporting the often-stated ambition of 'surveillance by consent'. The Commissioner has delivered a consistent stream of public engagement activities including facilitating public debates, media engagements and establishing a 'Surveillance Camera Day'[59] akin to an open day for surveillance camera control rooms. While measuring how the public responds to engagement activities often involves a level of uncertainty, and public opinion on surveillance acceptability is a notoriously complex[60] and overly politicised issue, it is reasonable to assume that such indicatives heighten public understanding of surveillance camera use in England and Wales.

By extension, public surveillance activities are more likely to gain legitimacy through such wider engagement. Reflecting on his experience, a previous BC attributed several features important to offering reassurance to practitioners and the public,

> *"The crucial elements to this reassurance are (1) they are exercised personally by the Commissioner who is independent of both government and the police and is personally answerable for the discharge of the statutory duties; (2) the Commissioner is publicly answerable through an Annual Report which is given to the Home Secretary, placed before Parliament and is published for all to judge how the Commissioner is exercising the statutory duties; and (3) the Commissioner is available to answer any questions from Parliament and the*

[57] Expressed in interview with the authors.
[58] Prof Paul Wiles, Commissioner for the Retention and Use of Biometric Material by the Police 2016-2020, unpublished submission to the original consultation supplied to the authors, reproduced with his kind permission.
[59] Surveillance Camera Day, URL: https://www.gov.uk/government/publications/surveillance-camera-day-20-june-2019
[60] E.g. Ditton, J. (1998) 'Public Support for Town Centre CCTV Schemes: myth or reality?', in C. Norris, J. Moran and G. Armstrong (eds.) (1998) *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate pp. 221-228; Gill, M. and Spriggs, A. 2005. *Assessing the impact of CCTV,* Home Office Research Study No. 292. London: Home Office. [Online]. Available at: http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf; Bradford, B., Yesberg, J., Jackson, J., and Dawson, P. (2020) 'Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology', British Journal of Criminology, vol. 6(6): 1502–1522

> *select committees but more broadly from the press and other media, pressure groups and individual citizens."*[61]

Notable here is the emphasis on a recognisable and publicly accountable individual with assigned responsibilities for this complex area of oversight. This is clearly something that will change with the erasure of this role.

Overall, the roles and functions of the BSCC in relation to surveillance cameras combines multiple statutory and non-statutory functions that intertwine and work together with the aims of: fulfilling statutory obligations; raising industry standards; providing guidance; and elevating public dialogue around surveillance. In this respect, the Commissioner has become a single point of contact for users, installers and the general public. This model of regulating public space cameras, based on policy and service co-creation, has been recognised as world leading and other jurisdictions, such as Belgium, Scotland and New Zealand, are considering a single point of contact for governance issues associated with surveillance cameras.

A senior local government representative interviewed for this report stated,

> *"The guidance and support provided by the Surveillance Camera Commissioner goes way beyond that offered by the Information Commissioner, in that his office provides clear guidance on 'best practice', the roles and responsibilities of local authorities and what are considered the best standards for running and managing public space CCTV systems… There is a definite advantage to having a single national source of guidance and support, especially for agencies like local authorities that struggle to acquire this knowledge."*

Alex Carmichael, Chief Executive of the SSAIB notes that whilst the SCCoP is not legally enforceable it carries considerable weight,

> *"It may not be enforceable legally, but it is enforceable as a piece of 'best practice', so if you are not following the Code, then what practice are you following? If you are in a Court of Law and you are asked, what guidance are you following and you say 'nothing', you have nothing to hang your hat on…it [SCCoP] is seen as the 'gold standard', so if you are not using it, the question should be why not and consequently how reliable and robust is your system?".*

The oversight of biometric material

Under POFA the 'Biometrics Commissioner' (BC) is required to: (1) keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints; (2) decide applications by the police to retain DNA profiles and fingerprints (under section 63G of the Police and Criminal Evidence Act 1984); (3) review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints; and, (4) to provide reports to the Home Secretary about the carrying out of these functions. Beyond these statutory functions the BC provides a single point of contact for guidance and advice relating to the governance of biometrics and considers how biometrics technologies and practices are merging with other surveillance technologies, especially in relation to surveillance cameras.

The Bill proposes the transfer of certain activities relating to DNA and fingerprints, specifically the transfer of PACE s63G and National Security Determinations casework to IPCO. No other biometrics oversight is required of IPCO by the Bill. The inclusion in the Bill of this direct transfer of functionality to IPCO is presumably because its inclusion in PoFA was a response to the European Court of Human Rights ruling against the UK on its retention of biometric data.

[61] Prof Paul Wiles, Commissioner for the Retention and Use of Biometric Material by the Police 2016-2020, unpublished submission to the original consultation supplied to the authors, reproduced with his kind permission.

Absent from the Bill are provision relating to the broader governance functions and roles of the Biometrics Commissioner.

Provisions in the Data Protection and Digital Information Bill relating to the roles and functions of the BSCC

Surveillance oversight is historically and currently overburdened and under-resourced. Activities undertaken by the SCC component have extended the Commissioner's role, not in terms of regulatory overreach, but to compensate for this shortfall, thereby raising standards and increasing professionalism across the sector. While not defined in the original legislation (POFA), these activities have arisen *as a result of successive Commissioners fulfilling their statutory duties*. The Bill proposes the erasure of all such surveillance camera-related functions and, by extension, disregards their associated value to society. As one expert interviewee for the report expressed, having been based on a consultation about 'absorption' of the functions by the Information Commissioner "*the Bill makes no provision for absorption whatsoever. It just deals with extinction*". For example, the Bill contains no provision for continuing the work of driving up standards for the development, procurement, adoption and use of surveillance cameras, a programme of work widely applauded across police, practitioner and industry communities.

Tony Gleason, Chairman of Public CCTV Managers Association stated for this report,

> *"Without the Code and the Commissioner, we could move into a scenario where surveillance and surveillance cameras are essentially used and operated by law enforcement agencies with their law enforcement priorities, and not local authorities with their broader community safety remit – where will local authorities go for advice in the future?... Since 2012 [the enactment of POFA] we have created something really useful [in the co-created SCCoP], we have developed it, nurtured it, and fine-tuned it so that it is an agreed industry standard…why would we want to 'throw it out', there will inevitably be a drop in standards, and there are no alternatives to replace it… A drop in standards will have consequences and will undermine public support".*

Tim Raynor, at the BSIA argued that,

> *"Without the guidance of the Surveillance Camera Commissioner, users and installers will not have access to guidance or support and will be forced to do everything themselves, this is especially the case in relation to procurement and as a result the technical specifications of systems will start to diverge with buying decisions determined by cost or the advice of consultants. At least with the Commissioner there was a standard reference point, a template to work from and ad hoc decisions were avoided.*
>
> *With the removal of the Surveillance Camera Commissioner, we will go back to the old ways, which was precarious. Those responsible for purchasing and installing camera systems will just have to make it up as they go along, these processes will become ungoverned, there wont be anywhere to go for expertise and support."*

Alex Carmichael, at the SSAIB further argues,

> *"As far as surveillance camera governance is concerned what we have [here] can be seen globally as best practice – a step-by-step method which puts in place the building blocks for accountable, ethical and effective surveillance camera systems…*
>
> *Without the Surveillance Camera Commissioner you will go back to the old days when it was like the 'wild west', which means you can do anything with surveillance cameras so long as you don't annoy the Information Commissioner…so, there will not be anyone looking at new emerging technologies, looking at their technical requirements or impacts, no one thinking about ethical implications – for emerging technologies like face-recognition, it will be a free-for-all."*

In current form, the Bill will delete all the surveillance camera-related oversight activities and mechanisms (and all but the aforementioned biometric casework activities) that are set out in legislation and arise from the fulfilment of statutory duties placed on Commissioners. Prominent among these is the tabled abolition of POFA legislative requirements to (a) appoint a SCC and (b) for the Government to publish a SCCoP, which offers governance coverage far beyond data-related issues. The removal of a legislative need to publish a SCCoP would also make the National Surveillance Camera Strategy irrelevant. This is likely to result in the lapsing of the ancillary activities connected to the strategy and designed to raise standards outlined above. This would include the removal of the Certification Scheme, the Self-Assessment Tool, the Buyer's Toolkit, the Standard's Group and associated training modules. The Bill contains no provisions for how these activities and functions will be fulfilled or maintained, which implies that the value of the Code and Strategy for providing surveillance oversight, raising standards in surveillance practice, delivering guidance for camera users, setting frameworks for future digital technologies, and offering transparency and public confidence is not recognised or seen as important.

The value of these activities, both statutory and non-statutory, are widely recognised and easily evidenced across civil society organisations, industry professionals, Parliament, and law enforcement communities. Of the latter, it is important to acknowledge significant evidence of police support for the SCC role, and requests for clarity over appropriate uses of surveillance tools. For policing agencies, the BSCC provides guidance, support and legitimacy for their use of overt surveillance camera systems. This in turn, gives them confidence that they have the legitimate democratic authority to use such systems where they comply with the SCCoP. The removal of the Code and associated requirements is likely to undermine this confidence and create uncertainly about how cameras should be used, and especially in relation to future policing developments.

Regulatory functionality

The BSCC's functions are not regulatory in the same sense as the Information Commissioner. The Information Commissioner and ICO have the legal authority and mechanisms at their disposal to conduct investigations and issue significant fines. The BSCC does not have these regulatory tools at their disposal and instead relies on co-regulation with stakeholders and the possibility of exposing poor practice to public visibility. This difference has several implications. First, the roles and functions of the OBSCC are not directly comparable with ICO. Consequently, the impact of BSCC functions arises through different and sometimes less visible or direct means. It also means elements cannot be directly 'lifted and shifted' into a different regulatory format and destination, as the ethos of regulation between the two agencies is fundamentally different. Also crucial is that the activities to be regulated extend significantly beyond matters of data use. In relation to surveillance cameras the BSCC takes a 'whole system approach' and considers technical matters, procurement, public awareness, etc, whereas the primary concern of the ICO are the data processes generated by surveillance camera systems.

A senior local government representative notes the flexibility in the approach offered by the BSCC,

> *"From an organisational point of view, we would not be keen on a more rigid regulatory model, the current approach is very sensible, it allows us to have a conversation, to work through issues and to find practical solutions."*

Tony Gleason, Chairman of Public CCTV Managers Association goes further, by arguing,

> *"Without the Code [the SCCoP] we [local authorities] will be dropped into the abyss...there will be a loss of knowledge about what constitutes the correct technical standards and practices, and we will be lost…the*

> *area will become unregulated and no one will be bothered until things go wrong…without the Commissioner there will be no appetite to continuously improve practices and technologies."*

Tim Raynor, Vice chair for the Video Surveillance Section, BSIA, argued,

> *"The ICO guidance is very much focussed on data and compliance with GDPR, whereas the Commissioner [the BSCC] covers a much bigger picture, for example how to buy a system, what are you going to do with a camera system, and how are you going to use it responsibly. The Code [SCCoP] filled this gap."*

Alex Carmichael, Chief Executive of the SSAIB argues,

> *"The other main regulator of surveillance cameras is the ICO and their main interest is the output of systems, the data they generate and process. This is just the output of camera systems, there is much much more that must be taken into account…for example…issues around why a camera system should be used when there may be alternatives, issues around the relationship between public agencies and commercial suppliers, issues around determining technical specifications, installation and procurement, not to mention ethical and privacy issues… The Information Commissioner's guidance on surveillance cameras is all about how to use the data in line with GDPR, it does not cover the technical information you need to set up a system, or the guidance around what you need to think about prior to establishing a system."*

One of the advantages of the 'whole systems approach' taken by the BSCC is that it recognises that the provision of systems necessarily involves collaboration with industry and that the involvement of industry in the development of the SCCoP is advantageous because it builds awareness and compliance. Alex Carmichael (SSAIB), explains this succinctly: "*Whilst POFA was targeted at public space surveillance camera systems, nine times out of ten, the people installing and maintaining them were from the private sector, so collaboration is essential if systems are to be delivered in the public interest.*"[62]

Examples of the impact of the BSCC

The reach and impact of the BSCC beyond core legislative requirements can be demonstrated by a couple of brief vignettes. These vignettes are examples of where interventions by the BSCC have resulted in changes to government policy or greater awareness of biometrics and surveillance camera issues.

Responding to the extended use of Automatic Number Plate Recognition Systems

Automatic Number Plate Recognition (ANPR) systems were developed and deployed as a response to successive Provisional IRA terrorist attacks in London's financial district during the 1990s. Implemented as one component of the wider security demarcation of the City, the so-called 'ring of steel', these deployments are credited as the first non-military uses of the technology in the world.[63] Over time, ANPR systems have proliferated, both within and beyond policing. They are now used for a range of law enforcement purposes, including the identification and tracking of serious offenders and for more mundane traffic offences. Beyond policing, this technology has become an important tool managing traffic restrictions, including bus lanes, monitoring traffic flows and enforcing Low Emission Zones (London Congestion Charge and ULEZ zones) across the UK. Within the commercial sector ANPR cameras are also regularly used to enforce parking regulations in supermarkets, shopping centres and other locations. The diffusion of ANPR cameras and systems over time has been both physical and also functional, from narrow policing priorities to broader issues around traffic management and climate change.

The scale of UK ANPR deployment is enormous. In 2021, the BSCC estimated that UK ANPR systems were eliciting 60 million matches per day.[64] In an interview for this report the previous

[62] Alex Carmichael interview for this report.
[63] Coaffee, J. (2003) *Terrorism, Risk and the Global City: Towards Urban Resilience*, London: Routledge.
[64] BSCC response to DCMS consultation.

SCC estimates that 100 million daily matches is a realistic assumption. The former SCC further stated that the UK ANPR database is the largest database in Europe.[65] As one founder member of the ANPR advisory group stated in an interview, "*when I first walked into the [advisory group] the stat was the Met ANPR database have had more photos than Instagram*".[66]

It is also important to note that ANPR databases can also comprise sensitive and personal information. Such increases in size brings changes in functionality and, consequently, proportionality, given unparalleled potential to track individuals across large distances via transport network cameras. For some critics, this represents a form of 'surveillance creep' as a technology designed specifically for once purpose has diffused into other settings for different initially unrecognised purposes. There are two further controversial aspects of these ANPR systems. Firstly, they have played a role in income generation for those agencies and companies using such systems, and for some this aspect is perceived to be more important than the service they are deployed to deliver. This has especially been levied at climate change and traffic mitigation schemes. Secondly, there are concerns about data matching processes and error rates with the National ANPR Service (NAS) estimating an error rate of up to 2%. In the context of 60-100 million matches per day, this translates into extremely high numbers of motorist being misidentified every day.

ANPR therefore represents an issue of where a technology has evolved in size and function to offer enormous surveillance potential. It has also become an issue of heightening public concern. It is notable that such developments occurred largely in a regulatory vacuum. ANPR expansion constitutes an example of how surveillance capability can develop much faster than the ability to regulate it. While different views exist over the role of legislation in response to such developments, such expansion foregrounds the absence of an explicit legal basis for different surveillance technologies that either represent step changes in surveillance functionality (such as FRT)[67] or scale (such as ANPR).

In the absence of such legislation, the intervention of the Surveillance Camera Commissioner can prove vital. This is particularly important given that the expansion of ANPR surveillance conferred risk on both the users and subjects of ANPR surveillance. In response to this regulatory gap, and the absence of an overall strategy for ANPR development, the previous SCC established an ANPR Independent Advisory Group (IAG) to bring accountability, raise standards and facilitate dialogue between key stakeholders engaged in disagreement of the role and future of the technology. Examples of outcomes include the better foregrounding of ethical considerations relating to new national ANPR Standards, assessment of the impact of cloned vehicles on the integrity of the systems and attention to error rates. This also provides an example of how oversight can support policing, rather than obstruct it. As one founder member of the ANPR IAG recalls at the inception of the group,

> *"As [the former SCC] said, the entire ANPR regime is one lawsuit away from it being totally struck down. I think that focused minds… The IAG was a space for critical friends, so it wasn't totally adversarial. But it provided a venue for sense checking, because, I think the Police hadn't really thought it through how long they were holding the data, who had access to the data and all that. So they did actually tighten up their policies and procedures… I think, all credit the police once they got over the shock of me said me sitting there, and [the former SCC], and the fear there was possibly a massive surveillance scandal in waiting going on here. You know, they, they were very good."*

This positive view of the IAG and its ability to expose surveillance users to critical voices in a

[65] Interview with previous SCC.
[66] Interview with Professor Lorna Woods
[67] For peer-reviewed academic research detailing the differences between surveillance cameras and FRT see Fussey, P., Davies, B., and Innes, M. (2021) "'Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing', *British Journal of Criminology,* 61(2): 325-344.

constructive way was echoed in an interview by the current chair of the IAG and NPCC lead for ANPR surveillance.[68] This development and the SCC-initiated IAG demonstrates the role the Commissioner can play in addressing regulatory gaps surrounding the accelerating growth of surveillance technologies, and mitigating the risks to both police and the public. While not set out explicitly in statute, such activities are nonetheless important for surveillance oversight. The abolition of the BSCC role will much reduce this oversight capability.

Addressing potential security risks brought by Chinese manufactured surveillance cameras

In September 2023 Parliament voted to approve a ban on installing Chinese-manufactured surveillance cameras from government, military and other sensitive sites. This move followed high profile political statements citing security risks from such technologies. For example, in a Parliamentary written statement on 24 November 2022, the (then) Chancellor of the Duchy of Lancaster (now Deputy Prime Minister) Oliver Dowden told MPs a review "*has concluded that, in light of the threat to the UK and the increasing capability and connectivity of these systems, additional controls are required*".[69]

The narratives surrounding these objections emphasise the potential for these devices to relay data back to China. Such data would include the personal data of UK citizens, and information relating sensitive sites include policing and national security operations. In addition, one of the world's largest surveillance camera suppliers, Chinese technology company Hikvision, has been shown to provide products with cybersecurity vulnerabilities which include the potential for cameras to be hacked and remotely monitored.[70] Less publicly commented on, but arguably as significant, have been credible reports implicating Hikvision surveillance technology in the racist widescale, systematic and enduring human rights abuses of Uighur Muslims and other minorities, most notably in the Xinjiang Uighur Autonomous Region.[71] Particularly problematic have been reports of the deployment and finessing of these products in detention centres[72] and, separately, offering ethnic profiling capabilities.[73]

The above political interest in this topic is a direct result of persistent and committed campaigning by the BSCC on these wider range of concerns. Since 2021 the BSCC has played a principal role in evidencing the extent of Chinese manufactured surveillance cameras from public places and government buildings in the UK, and then leading calls for a ban on such devices, referring to these surveillance tools as 'digital asbestos'.[74] The success of this approach relies on the BSCC focus on a 'whole system approach' including matters relating to human rights, procurement, cybersecurity, technical specifications and data processes. The BSCC also leveraged his position to canvas police forces on their procurement of Chinese-manufactured surveillance apparatus to surface the extent of the problem, revealing that the majority of forces surveyed had adopted equipment from corporations associated with security, ethics and rights-based concerns.[75] Overall, as a direct consequence of the intervention of the BSCC the UK has banned the procurement and deployment of new Chinese surveillance cameras and has encouraged the removal of existing systems.[76] A local government representative commented for this report,

> *"We've been talking to him [BSCC] about the complex issues associated with procurement of cameras produced by firms in foreign states which have implications for the Surveillance Camera Code and data protection, because of the vulnerabilities that Councils may find themselves in if they have procured*

[68] Interview with Chief Constable Hall.
[69] Written statements - Written questions, answers and statements - UK Parliament
[70] See IVPM (2018) *Hacked Hikvision IP Camera Map USA And Europe*, available from https://ipvm.com/reports/hik-hack-map.
[71] Amnesty International 2018 https://www.amnesty.org/en/latest/news/2018/08/china-systematic-repression-of-ethnic-minorities-laid-bare-in-un-findings/; Uighur Tribunal 2021
[72] https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html
[73] https://www.theguardian.com/world/2022/dec/04/chinese-security-firm-advertises-ethnicity-recognition-technology-while-facing-uk-ban
[74] UK policing 'shot through' with Chinese surveillance technology - GOV.UK (www.gov.uk)
[75] Ibid.
[76] UK government bans new Chinese security cameras - BBC News

> *equipment with no guarantees that the data being generated is entirely secure and because there are risks it may end up outside the UK."*

The adoption and amplification of this issue, demonstrates the agility of the BSCC role in addressing emerging issues of public interest and concern. It also further underscores the argument that regulation and oversight can facilitate security, rather than obstruct it as this issue is traditionally framed. Moreover, this episode provides evidence of how agile systems of oversight can anticipate emerging harms and bring them into political and public consciousness.

PART THREE:
ANALYSIS OF PROPOSED ABOLITION OF THE BSCC ROLES

This part of the report presents an analysis of the proposed changes to the BSCC arising from relevant provisions embedded in the DPDI Bill. This is organised around the core functions of the BSCC, the main lines of argument for the abolition of the BSCC and key themes emerging from the empirical research supporting this report. The main lines of argument presented here are evidenced in the direct words of those interviewed.

Simplification

Current oversight of complex surveillance practices are widely considered as patchy and requiring simplification. Such sentiments are expressed by a range of different bodies and are prominent in the recent House of Lords Justice and Home Affairs Committee review of digital policing[77] and the independent 2022 Ryder Review[78] legal analysis of biometric governance. As stated in the latter,

> *"The introduction of a new legal framework should simplify rather than complicate, the existing patchwork of statutory bodies overseeing the law and regulation of biometric data. We were struck by numerous witnesses expressing concern over potential confusion over which commissioner or regulator had key responsibility over the safeguards relating to a new technology and how overlapping roles were resolved… In the absence of a clearer oversight structure, the numerous codes of practice or guidance notes issued by different public authorities at various times create confusion, rather than clarity."*[79]

Simplifying oversight has been consistently stated as a key aim for the Bill. However, and as highlighted across this report, many calls for simplified oversight correctly include a requirement for companion policies to support implementation and compliance. Such policies play a vital role in translating abstract principles into clear guidance and standards for users of biometric and other surveillance technologies while offering mechanisms for auditing compliance. By contrast, the requirement for the government to publish an explicit surveillance camera focused Code of Practice (SCCoP) already exists through POFA yet is to be deleted by the Bill. The absence of requirements to provide guidance and to ensure compliance generates vulnerabilities for users of these technologies and for the rights of individuals subjected to them. Moreover, given the pace of technological change, such policies and codes are one means to provide an agile response to the significant uncertainties brought by emerging technologies.

Simplification and depletion

Several expert participants highlighted that simplification is an important ambition, yet it should not come at the expense of meaningful oversight. For example, a former Surveillance Camera Commissioner questioned,

> *"Why is it all of a sudden, that simplification is more important than raising standards? And the role of the commissioner has been to introduce relevant certification to provide guidance on facial recognition to oversight of ANPR. None of which would necessarily fall under ICO, ECHR or anybody else."*

Taking the case of facial recognition, the main interventions offered by the main bodies tasked with oversight of this technology under the 'simplified' arrangements proposed by the Bill[80] – the

[77] House of Lords, Technology Rules… https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf
[78] Ada Lovelace Institute (2022) *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, P71-72 available from https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf
[79] *Ibid.* p.66-67
[80] As stated by the Government in the guidance notes accompanying the Bill and in explanations offered during the Commons Public Committee Stage. The Bill itself is silent on where these functions might go.

ICO and the EHRC are (a) a 2019 opinion published by the (then) Information Commissioner[81] and (b) a position piece by the EHRC.[82] The former called for a legally binding code to govern the use of facial recognition technology while the latter called for a suspension in the use of this technology. Both have been ignored. Indeed, the only detailed guidance addressing uses this technology, and that places it in its legal context, was issued by the Surveillance Camera Commissioner in 2020,[83] the oversight body the Bill seeks to erase.

Further depletion of oversight is outlined by the Scottish Biometrics Commissioner. Key here is the comparison between the oversight of biometric materials in Scotland compared to arrangements for England and Wales. Biometric oversight arrangements in Scotland are tied to the law on criminal procedure. Suggested changes to oversight in England and Wales propose removing points of independent oversight,

> *"This all comes back to the purpose of the primary legislation. My function in Scotland relates to the Criminal Procedure Scotland Act. So we're actually interested in the effective lawful and ethical use of biometric data as it relates to domestic criminal procedure law. In England and Wales, it's more about Protection of Freedoms. And it just seems to me that this move [the Bill] seeks to diminish those protections. I know the role of the Biometrics Commissioner for England and Wales is about all sorts of other things. But it was wrapped up or framed in terms of protecting people's freedoms and human rights…*
>
> *And I'm afraid that I think this is part of a wider agenda. I do think it's tied up with a sort of take back control after Brexit agenda, let the police do what they want. Get all these pesky risk regulators out the way because they just end up criticizing government policy. I know, that's an oversimplification but that's how I see it. So I see our function in Scotland, this links to domestic criminal procedure of legislation. Fraser's role in England relates to protection of freedoms. The ICO across the UK relates to data protection and information rights. These are three very different but mutually complementary roles. And if you strip out one of the really big ones, the BSCC, I think it's a backward step."*[84]

Similar to the discussion on the FINDS-SB board the BSCC role is considered here as one that interfaces with other forms of oversight, rather than replicating them. Removing these functions therefore generates considerations of how other forms of oversight are balanced and constituted.

Simplification and the relationship between oversight bodies

How the BSCC relates to other oversight bodies, and the impact of deleting the former role, therefore constitutes an important question. Three considerations are particularly relevant here: (1) the relationship between standards, handling and oversight of biometric materials; (2) constitutional matters regarding devolved administrations; and, (3) the activities of organisations that have hitherto been uninvolved in surveillance oversight.

Taking these in turn, it is important to recognise the relationship between the BSCC and other regulators. For example, and with regard to the Forensic Science Regulator (FSR), the FSR sets standards for producing DNA and fingerprint profiles while the BSCC has oversight of the process. The latter includes whether the DNA should be retained in the first place and how the information is used. The Forensic Science Regulator elaborates on this relationship in a written submission to the authors,

[81] ICO opinion October 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
[82] Equality and Human Rights Commission (2020) Facial recognition technology and predictive policing algorithms out-pacing the law, available from https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law
[83] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf
[84] Interview with Scottish Biometrics Commissioner

> *"The FSR and Biometrics and Surveillance Camera Commissioner have separate but complementary statutory remits in terms of the use of forensic and biometric data in the investigation of crime and criminal proceedings. Our overarching goal is to ensure the accurate, reliable and legal evidence is used and that community confidence is maintained in the criminal justice system and the use or forensic and biometric data by the state. There are significant risks to the illegal, inappropriate or erroneous use of biometric data and these are not theoretical as the various reports produced by the FSR and Biometrics and Surveillance Camera Commissioner have outlined. By working closely together and through the broader governance of FINDS Strategy Board the FSR and Biometrics and Surveillance Camera Commissioner can take a "whole system" governance view addressing issues as they arise and anticipating developments in science and technology so that safeguards are built into the regulatory structures that apply to the use or forensic and biometric data".*[85]

As such, while both the FSR and BSCC attend to a similar issue, the two roles are better seen in terms of complementarity. From the perspective of the FSR, this complementarity is mutually beneficial. It allows a 'whole system' approach to this complex area of governance and offers capability to address the range of concerns, rather than constituting duplication. Removing the BSCC from this equation may, therefore, hold implications for the handling of biometric material and, as a corollary, complicate rather than simplify the process.

Another complexity brought by the arrangements proposed in the Bill affects devolution. The current BSCC highlights concerns relating to the relationship between England and Wales, and with Scotland,

> *"In terms of the devolution aspect of this, they will have significantly complicated it. Because if this is all to be treated as data protection, which it is from the bill, then public space surveillance by the police will be a reserved matter. This means that, in Scotland, the Biometrics Commissioner, who is just about to be to be invited to include public space surveillance for the same reasons we have,*[86] *we'll be dropping it at the same time. And you have complicated that system in Scotland. And then, if you carve out Scotland as being an exception, so they can have their own commissioner to do public space surveillance [e.g. instead of the ICO], you've complicated it again. It isn't simplification. Whatever it is, they need a better descriptor for this."*[87]

From a constitutional perspective, part of this complexity arises through the different jurisdictions of the related agencies. As noted in Annex II, the ICO operates at the UK level, EHRC in Britain, the Investigatory Powers Commissioner covers the entire UK, the BSCC covers the UK for the purposes of National Security Determinations and England and Wales for all other functions, and Scotland has own Biometrics Commissioner who will, even after the Bill's enactment, have no oversight of National Security Determinations made by the Chief Constable of Police Scotland. While an argument can be made that housing these functions in IPCO and a reconstituted Information Commission erases problems because both hold a UK-wide remit, it does not necessarily simplify the work of existing bodies. In fact, responsibility for approving applications by chief police officers to retain fingerprints and DNA profiles for non-National Security cases only applies to England and Wales and will probably be the only function of the Investigatory Powers Commissioner to be so restricted. Neither does the Bill simplify the work of other existing bodies that will remain in place once the Bill becomes law.

As the Scottish Biometrics Commissioner describes, his role was established by legislation that explicitly references the Protection of Freedoms Act (albeit in limited way). In reality, the practical delivery of statutory duties for both SBC and BSCC roles has been achieved through liaison. The Scottish Biometrics Commissioner elaborates on this relationship,

[85] Written submission from the Forensic Science Regulator.
[86] The Commissioner is referring to the merger of the two POFA Commissioner roles – the Surveillance Camera Commissioner and Biometrics Commissioner – in 2021.
[87] Interview with the Biometrics and Surveillance Camera Commissioner

> *"We've tried to work as closely as we can. The commissioner for England and Wales is referenced in the Scottish legislation. The postholder is one of the bodies whom I must consult with when preparing the Statutory Code of Practice in Scotland. This has had legal effect in Scotland since 16th November last year. I am required by the Scottish legislation to have a professional advisory group and [the BSCC] sits on that. We both sit together on the UK FINDS Strategy Board, which is a UK strategic oversight board chaired by a deputy chief constable that oversees the running of the UK DNA and fingerprint databases. It also oversees how their exchange mechanisms work. The ICO also attends that forum, but for a completely different purpose. All of this is about layers of governance and accountability within that kind of complicated UK infrastructure.*
>
> *Interviewer: So, is there a point here that, in order to assist or even fulfil your legislative obligations, there's this kind of liaison with the BSCC role?*
>
> *Yes. Absolutely. And that is, that is also specifically because in the Criminal Procedure (Scotland) Act of 1995 there's a provision to grant authority to the Council,[88] as it was, then aim to oversee in the retention of fingerprints and DNA under a national security determination in Scotland. So, the two pieces of legislation reference each other if that's not the wrong way to describe it."*

Relatedly, the Scottish model for the oversight of biometric material was recently singled out as an example of good practice by the Ada Lovelace Institute's review of biometric regulation. Noting that the legal requirement to follow the Scottish Biometric Commissioner's code provided greater regulatory scope and, crucially, clarity for decision-makers.[89]

Relationships between Biometrics and Surveillance

Further possibilities for complicating the oversight landscape exist. The relationship between covert and overt surveillance activities, as discussed below, is relevant here. Here, the growing capability and intrusive potential of surveillance technology is likely to further complicate the distinction between overt and covert uses of such tools. Another element concerns the 2021 combination of the formerly separate Surveillance Camera and Biometrics Commissioner roles under one public appointee. It would appear that, ostensibly, this was adopted to bring unified oversight across both areas in the context of advancing forms of biometric surveillance; notably reflecting the fact that areas such as facial recognition technology straddle both biometrics and surveillance. The BSCC considered that the result of the Bill's erasure of this role on the way surveillance and biometrics are dealt with coherently will be that,

> *"We will split them into two and send them to two different places. Even though we, our policy, and our ministerial approach has been that they need to be in the same place. Two sets of two of interrelated functions that are currently managed and overseen in one place will be split. And you're saying this is for the purposes of simplification?*
>
> *Surely the better answer is to say, "well, this is growing and growing and growing, in which case, we'll all follow the same rulebook." And that's not what they are saying, which is that it will all reduce to its minimum component parts of data processing. And in doing so we're going in the wrong direction… And one of the things that struck me is how much of my time in this role I've spent talking to other countries where they say, oh, we need one of these. Can you tell us what you do?"*[90]

Adding to this complexity is the role of organisations that have previously not operated in this manner or addressed such matters in comparable depth. As detailed above. The reconstituted

[88] The Criminal Courts Rules Council, established under s304 of the Criminal Procedure (Scotland) Act 1995. This body oversaw the procedural matters that covered the handling of biometric material (s. 304(9)(a)).
[89] Ada Lovelace Institute (2022) *The Ryder Review.*
[90] Interview with Biometrics and Surveillance Camera Commissioner.

ICO would require significant investment and capacity building to address the functions currently undertaken by the BSCC.[91] It would also require a shift (and extension) in the role and purpose of the EHRC. Added to this is ensuring expertise that exists with the BSCC role is retained:

> *"So, the idea of simplifying…you are just going to have a far bigger, more complex organisation. You get rid of Fraser Sampson, but then you'll have to have a Fraser Sampson, in these organisations or someone doing that. So I don't see how it's simpler. I'm trying to make the point that in these regulatory bodies, these issues are not covered. So the fact is they're gearing to have to introduce this expertise. I'd say it just adds, you're just making those organisations more complex. One of the ironies of this is that in pursuing what they are describing as simplification is actually complicating. And in a world that is struggling already with too much."*[92]

Several senior police officers also raised the point that removing such expertise will generate complexity. For example,

> *"I think there's some huge complexities there. There's a, there's a huge amount of projects and lack of joined up thinking around producing systems for law enforcement around CCTV… So one of the huge issues we've got at the moment and this, this isn't just in the analytics space, it's in the viewing space, it's in the processing space and the enhancement space. Is that nobody out there other than those actually working with CCTV have an understanding of the complexities of CCTV. Yeah. And I had this conversation yesterday with some of the guys at the [one project] saying that you've got 300,000 different formats of CCTV out there at the moment. You know, you can have a CCTV manufacturer producing a model of CCTV system that will take anywhere between four and 47 cameras attached to it. Every single installation of that particular make and model or system will be different because the configuration for each camera can be particularly different. So then when you actually export that data from those camera systems, every single export will be different in its configuration. So it's not just what's on the video stream. One of the things that we've been trying to get across to a lot of these projects is, you know, you can get the top it people in from across the world, and they will still have a huge problem in just ingesting the data in the first place, let alone processing it."*[93]

Another senior police officer with a national leadership role for CCTV elaborates on this point,

> *"I think for me simplification is a strange objective, in what is an increasingly complex area of business. Things may or may not be more complicated under the new arrangements. But I suspect they will be not just more complicated but probably less effective as well. I think what's needed is a more system wide view. And I don't think we get that. I'm not sure we would get it at all. I also feel we don't need more simplification here. I don't think that's anything that any of us would be would even have thought of asking for."*[94]

Practical implications

What may appear a simplification in organisational terms does not naturally translate into simplification in a practical sense. As stated above regarding the proposal to vary oversight of different biometric materials, this ambition for simplification may actually generate regulatory complexity. Removing a Commissioner who proactively interfaces with developers and users of surveillance technologies, is underpinned by a legal code of practice published by the Government, and whose role is widely supported by these practitioners may generate future difficulties. For example, it may take longer for aspiring technology users to access knowledge or for standardised technical specifications to emerge. In addition to impacting public resources, pressing ahead with surveillance deployments before such advice is received may generate greater

[91] Stated in the ICO response to the original Bill Consultation https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf
[92] Interview with Biometrics and Surveillance Camera Commissioner.
[93] Interview with Andy Read, South Wales Police, National Police Chiefs' Council National Capabilities Manager for CCTV
[94] Interview with Assistant Chief Constable Jenny Gilmer, South Wales Police, National Police Chiefs' Council lead for CCTV

exposure to litigation for public bodies. Alternatively, and from a public safety purpose, the absence of such information may lead users to highly conservative interpretations of the law which may dissuade legitimate uses of surveillance technology for public safety.[95]

Removing the BSCC could generate complexity in other areas. As set out in Part Two, the BSCC plays a major role in engaging with the public and practitioners on surveillance-related issues. The current postholder highlights the likely impact on this activity,

> *"I think it will be a much harder to measure cost, which would be back to trust and confidence and public satisfaction. I reckon probably a quarter of the journalists who come to me come because nobody else would answer them. There won't be any new people to answer these questions. Where will they go? I think where where you haven't got that that route in then there is a risk of just creating another frustrating world. People have got very genuine and important questions. Those questions are made even more important if you're going to rely on them as policing does in relation to consent."*[96]

The value of the BSCC knowledge brokering role, and impact of its loss, is further highlighted by the Forensic Science Regulator who, reflecting on the 'invaluable' advice received during a challenging issue arising his tenure chairing the FINDS board,

> *"I found myself as the chair resisting a determined legal challenge by a council social services department to use DNA profiling data collected under PACE to establish the paternity of a child in a civil custody case. This was not an isolated incident and I can envisage other situations with the wider use of biometrics including fingerprints, DNA and face where the data held for the purposes of investigating crime, eliminating individuals from investigations and bringing offenders to justice will be the subject of challenge to access this data to be used for other purposes. While I made the decisions as the Chair and would have gone to court to resist the challenge I found the advice of the members of the strategy board including the Biometrics Commissioner invaluable in how I dealt with this and similar situations".*[97]

Reduced public engagement on issues of surveillance and biometrics is one potential consequence of the plan to erase the BSCC role. Limiting access to information may hold further implications. Among other effects, the BSCC considers that this would disrupt the opportunity to raise standards when surveillance camera users are installing systems. This could lead to hidden downstream costs for installers,

> *"But I think there are a number of potentially hidden costs. One would be an economic one. It will take longer to get to an answer or to get to some help. This is one of the biggest areas of growth and we need the accountable public use of equipment. So it reach a point where the other places people seek information, the other doors you'll have to knock on... I already have very long queues of people seeking advice. And so to break this up, and then expect people to join that queue will have its own cost, from the opportunity costs and delays. And it may also have cost because people can't wait for an answer, so they just do it and see what happens."* [98]

This point of engagement would also disappear at the same time as the dismantling of the Third Party certification scheme designed to support surveillance camera users through the process of installing systems. For one academic expert, reducing access to guidance and expertise on standards not only risks harming public trust and confidence, it may also expose surveillance camera users to vulnerability from litigation,

---

[95] See Fussey, P., and Sandhu, A. (2022) 'Surveillance Arbitration in the Era of Digital Policing', *Theoretical Criminology*, 26(1): 3-22 Open Access available here

[96] Interview with Biometrics and Surveillance Camera Commissioner.

[97] Written submission from the Forensic Science Regulator.

[98] Interview with Biometrics and Surveillance Camera Commissioner.

> *"At least pluralistic oversight through these different commissioners and their offices allows for input into how the police use new technologies and more specialist guidance to be developed. If you chop that away and replace it with nothing, I think you are stripping away a layer of accountability and oversight that at least serves as some kind of buffer between free virtually unrestricted police experimentation and the slow legal challenge, possibly 10 years later. The Commissioners each in their own way, seem to mediate and to work with police forces who often welcome this regulation, oversight and guidance. They [the police] are not necessarily institutionally set up to take account of all these different issues themselves, but they will work with commissioners, even if they do not agree with them, on these issues. Stripping that away and replacing it with nothing, seems to invite future legal challenges and conflicts down the line"* [99]

This point also links to the accounts in Part Two detailing the positive perception of both the BSCC and its wider function by the police and other surveillance camera operators.

Future proofing

The Bill seeks to transfer some responsibilities outlined in POFA (fingerprints and DNA profile retention in certain circumstances) to IPCO, allow others to lapse, and makes no provision to the functions and oversight activities arising from several POFA Commissioner duties. One argument has been that many SCC activities are not defined in POFA and therefore cannot be transferred. As noted in Part One, one likely explanation for naming DNA and fingerprints in the Bill is that they are specified in the Protection of Freedoms Act, in part as a response to a European Court of Human Rights ruling against the UK on the retention of DNA data.[100] However, POFA further established the Government's SCCoP and enables the SCC to provide and issue guidance across the surveillance landscape. It also requires 'relevant authorities' to comply with the principles of the Code. These are two powerful requirements which hold state actors to account.

Authored over a decade ago, POFA referred to just two forms of biometric material: DNA data and fingerprints. The Bill makes no reference to practices that have since developed and, therefore, the limited transfer of biometric oversight (on PACE s63G and National Security Determinations concerning the retention of biometric material) to the Investigatory Powers Commissioner remains focused solely on these two biometric materials. There is merit in utilising the IPC role in this regard given IPCO undertakes additional functions concerning authorisation and inspection. The original proposal consulted on was for all POFA biometric and surveillance oversight functions to be transferred to the ICO. However, the Bill reflects a perspective that some biometric casework sits more naturally with IPCO but it leaves the remainder of the functions in relation to both biometrics and public space surveillance unaccounted for beyond generic data protection considerations.[101]

Designating retention decisions focused solely on fingerprints and DNA to the Investigatory Powers Commissioner also risks a de facto segregation in the oversight of different biometrics techniques. Some (decades old) biometric materials will be brought under an explicit regulatory regime while the oversight of unnamed and emergent forms become more ambiguous. This segregation also places varying emphasis on different forms of biometric material. Distinct statutory obligations are assigned to the oversight of fingerprints and DNA (and, anachronistically, footwear impressions[102]) and, accordingly, regulatory attention must fall on

---

[99] Interview with Dr Joe Purshouse.
[100] *S and Marper v United Kingdom* 30562/04 [2008] ECHR 1581
[101] It is worth restating that this approach is at odds with that taken in other advanced democracies. For example, despite establishing what was at the time the most far reaching data protection arrangements in the world under the GDPR, the EU is in the final stages of ratifying the AI Act (Draft). This contains several surveillance-related provisions, including explicit focus on facial recognition technology, and therefore demonstrates clear acceptance that data protection is an insufficient frame to address the range of potential impacts in an ago of advanced AI driven surveillance.
[102] See s.61A of the Police and Criminal Evidence Act 1984.

these aspects. Unmentioned forms of biometric material become merged into in a less specific body of oversight activity.

This prospect of splitting biometric oversight across organisations has been present since POFA and, in that sense, is not new. The potential for unequal oversight of different biometric materials is also a consequence of developing legislation in the manner that it has, as a piecemeal response to legal challenges to erstwhile practices (see Part 3). The Bill also removes oversight of retention and use of DNA and fingerprint profiles that are not retained under s.63G of PACE or subject to a National Security Determination. Moreover, considerable differences exist over the impact of advanced surveillance technologies and biometric techniques in 2023 than in 2012. Specifying only those biometric techniques mentioned in legislation of over a decade ago challenges notions that the Bill is 'future proofed'. Accordingly, genuine and meaningful future proofing would likely take account of such differences.

Implications for regulation

The proposal to assign some retention decisions for DNA and fingerprints to the Investigatory Powers Commissioner while leaving others unnamed may generate additional complexities for regulators. As such, abolition of the BSCC role will *complicate* the work of existing regulators. As the Forensic Science Regulator explained in a written submission for this report,

> *"I am aware of the changes proposed in the Data Protection and Digital Information Bill but no detail of this or an impact assessment on the overall governance of the use or forensic and biometric data has been shared with me. My observation would be reflecting my response to [author's question on impact of abolishing the BSCC role on the governance and oversight of biometric materials] is that if the intention is to take a minimalist approach to cover off only those things that are statutory requirements then the lack of a joined up whole system view and the interactions I have had both ways with the Biometrics and Surveillance Camera Commissioner will mean a significant degradation in the governance and oversight of forensic and biometric applications. With respect to the direct impact on the FSR role, this has now been put on a statutory footing under the FSR Act 2021 and in the first statutory Code of Practice I have defined the management of forensic databases as a forensic science activity that will be subject to the statutory Code. This was a specific requirement set out in my terms of appointment and I was anticipating the Biometrics and Surveillance Camera Commissioner making a significant contribution to the development of the regulatory framework for forensic databases".*[103]

Two observations over the impact of abolishing the BSCC role are particularly important here: the sense that the oversight of surveillance cameras and biometric materials will experience '*significant degradation*', and the additional difficulties this will introduce into the FSR role.

On a related issue, the importance of having the capability to update and integrate the focus of biometric oversight were expressed by an academic expert,

> *"We have the Protection of Freedoms Act, which occurred quite a while ago, before this [form of] facial recognition came about. But we've all recognised that the issues around facial recognition and so forth, that we've never had to deal with this sort of stuff before. We've previously dealt with very similar, if not the same issues when it came to retaining people's fingerprints and people's DNA. So of course, it made perfect sense that we would try and implement oversight transparency that were in line with what we did with DNA and fingerprints. So to me, to split them up again makes absolutely no sense."*[104]

[103] Written submission from the Forensic Science Regulator.
[104] Prof Carole McCartney interview

Added to this is the view expressed by a former Biometrics Commissioner that "*reference to only fingerprints and DNA in legislation has always been insufficient.*"[105] The relevance of this view for current forms of biometric surveillance is evident from the only UK legal proceedings addressing facial recognition technology.[106] This judged against the excessive discretion given to individual police officers using this technology. Explicit guidance and oversight, therefore, not only serves to protect the rights of citizens, but also offers certainty and other advantages for technology regulators and users.

Of further note is how the Government's SCCoP, intended to be scrapped by the proposed legislation, has provision for emerging forms and novel uses of technology. For example, the Code calls for more in-depth risk assessments in circumstances where *"[i]n general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy."*[107]

Implications of emerging technologies

Biometric monitoring technologies are expanding and diversifying at an unprecedented rate. These new capabilities have significant scope for intrusion. While uncertainty will always exist over some technological futures, others are not difficult to ascertain. For example, the Minister of State for Crime, Policing and Fire's ambition to embed facial recognition technology in policing and pursue how the Government can do to support the police on this was recently revealed by the BSCC in the interim version of this report (see Appendix I).[108] Such 'embedding' is extremely likely to include exploring integration of this technology with police body worn video (interview with the BSCC) and potentially drone capabilities as each technology develops. A case for designated oversight for this technology has been made elsewhere. Here experts and public bodies have called for more detailed rules for uses of this technology in public.[109] Academic research has also demonstrated significant public concern over public uses of this technology. [110] A stark contrast exists in the working of the Bill between mention of relatively uncontroversial decades old biometric techniques (DNA and fingerprints) and the cutting-edge technologies currently animating public debate. This point has added significance given current concern over declining levels public trust and confidence in the police and their importance for maintaining legitimacy.[111]

Facial recognition is one of many evolving surveillance capabilities. Innovations in voice recognition and claimed advancements in emotion and sentiment analysis[112] are examples of rapidly growing forms of biometric surveillance. Several participants highlighted concerns over the growing use of surveillance drones amid a lack of formal regulation. For example, The Deputy Mayor for Policing and Crime for West Yorkshire commented,

> *"I think there are massive human rights implications of drones. So there are currently lots of forces using drones. So we [West Yorkshire] are the national lead for the National Police Air Service. This includes helicopters, and the surveillance cameras in helicopters. What is going to happen to the oversight of all that? The surveillance footage is so high definition that you can literally see in people's gardens, you can see people sunbathing and all the rest of it."*[113]

[105] Unpublished Biometrics Commissioner's Response to DCMS Consultation supplied to authors by the previous Commissioner.
[106] R (on the application of Bridges) v Chief Constable of South Wales Police. It is also relevant that a July 2023 European Court of Human Rights decision (*Glukhin v. Russia* App no 11519/20 (ECtHR, 4 July 2023)) classified retrospective facial recognition and live facial recognition as intrusive and therefore necessitating a high level of justification for their use. Accordingly, it is likely that, at a minimum, they would treat biometric data gathered through facial recognition as deserving equivalent protection as fingerprints.
[107] 'Surveillance Camera Code of Practice Pursuant to Section 20 of the Protection of Freedoms Act 2012', Home Office, para 2.2.
[108] UK policing minister pushes for greater use of facial recognition | Financial Times (ft.com)
[109] *Inter alia* Ada Lovelace Institute (2022) *The Ryder Review*
[110] Bradford et al., BJC; Murray, D. (2023) in press
[111] UK Parliament (2023) Trust in the Police, https://researchbriefings.files.parliament.uk/documents/POST-PN-0693/POST-PN-0693.pdf
[112] The efficacy of emotion recognition technologies is subject to considerable debate (Maguire, M. and Fussey, P., (2016). Sensing evil. Focaal. 2016 (75), 31-44).
[113] Interview with Deputy Mayor for Police and Crime, West Yorkshire.

New challenges brought by increasing uses of airborne surveillance include questions of proportionality and collateral intrusion. Moreover, using such tools without clear understanding of the legal framework may generate costs in terms of public trust and legitimacy, as evidenced in Derbyshire Police's decision to use drones to publicly 'shame' law abiding hikers during the pandemic.

Additional to this is the increasing integration of visual surveillance with other forms of data and monitoring. As one academic expert stresses,

> *"My more general concern is the loss of anonymity. This is my point about privacy and public spaces. We're getting drones with automatic facial recognition, better quality on ANPR cameras, also obviously mobile phones and telemetry, body worn. I think by seeing by seeing them as separate you don't see the cumulative effect. And I think that's an issue because moving into digital recording of things means that you're able to combine different data sources much more easily."*[114]

While data-focused practices are increasingly brought into broader surveillance activities, debate exists over the sufficiency of data protection legislation to offer meaningful oversight of the range of surveillance possibilities (see Part 3). The previous Surveillance Camera Commissioner highlights this point in a briefing paper supplied to the authors,

> *"The Data Protection Act 2018 (DPA) has future capabilities within its scope so far as processing personal data is concerned. To consider that this legislation on its own will provide sufficient legitimacy and effective regulation of the use of evolving surveillance capabilities may be a tenuous assumption."*[115]

What is notable about such technological advancements is not only the increasing capabilities of surveillance techniques – and hence the need for oversight – but also the merger of surveillance and biometric capabilities. The segregation of biometric material in the Bill also potentially removes any explicit statutory duties from the interface of biometrics and surveillance, the policy basis on which the Commissioner functions were combined under one appointee in 2021.[116] This was same year the Government released a consultation on its proposed abolition of both roles (without prior consultation with the post holder).

Given the considerable public debate and legal attention to remote biometric monitoring technologies such as facial recognition, and the way they have been addressed in other countries, this omission is surprising. Attention to existing, near future, and likely developments 'just over the horizon', and thereby establishing clear responsibilities for overseeing technologies of significant public concern, could invest the legislation with further specificity, purpose and sustainability. Rather than specifying each technique, one approach could be to categorise these technologies in a very broad sense that ensures future relevancy, such as 'remote biometric monitoring'. Moreover, one could argue that given the potential for collateral intrusion, remote biometric surveillance resonates more closely with IPCO's remit than decisions to retain fingerprints and DNA in a small number of exceptional cases (the latter being arrangements proposed under the Bill).

Developing challenges: covert and overt surveillance

One consequence of advancing technology is the growing ambiguity over any boundary between overt and covert surveillance. It is likely that this issue will become more pronounced in the coming years. The Government position is that a comprehensive legal framework addresses directed and covert uses of surveillance, such as Regulation of Investigatory Powers Act 2000 and

[114] Interview with Professor Lorna Woods.
[115] Anthony Porter, former Surveillance Camera Commissioner, Futures paper provided to the authors.
[116] Interview with BSCC

the Investigatory Powers Act 2016. A complication here is the growing intentional and unintentional potential for overt surveillance measures to be used in a covert manner. For example, advances in facial recognition technology increasingly allow for overt surveillance camera feeds to be used for directed surveillance. A clear example of this can be found in a 2019 Investigatory Powers Tribunal judgement, *AB V Hampshire Police*. The Tribunal's judgement and reasoning resonates with many of the issues discussed here. Most notably, the Tribunal judged that surreptitious police use of (normally overt) Body Worn Video surveillance while interviewing a homeowner about a domestic burglary was capable of amounting to "surveillance" for purposes defined in Part II of RIPA, and hence in a covert way that would require authorisation.[117] This case also further demonstrates the way camera surveillance issues extend beyond matters of data protection.

This point concerning the covert use of overt surveillance tools is also articulated in a briefing paper prepared by a former Surveillance Camera Commissioner,

> *"Overt surveillance camera systems can very quickly be intentionally or unwittingly operated in a manner which causes the surveillance being conducted by it to become 'covert' in nature and therefore requiring of an authorisation being granted under the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA)…*
>
> *The covert use of overt surveillance camera systems is not an uncommon occurrence particularly in respect of local authority owned CCTV and indeed the police use of ANPR. The Investigatory Powers Commissioner's Office (IPCO) provides regulatory guidance on such matters…*
>
> *The following excerpt from the first Investigatory Powers Commissioner's annual report similarly has relevance: "On occasion, public authorities conduct 'non-RIPA' surveillance because an authorisation, whether directed or intrusive, is unavailable under the Act. This could include, for example when the police, by consent, seek to deploy a camera within the house of a vulnerable person in order to investigate allegations of doorstep 'scams'. Authorities need to be careful in these circumstances, to ensure that the activity is appropriately overseen. This will often include implementing a non-statutory authorisation process that runs in parallel to any RIPA approvals. We will review the adequacy of these arrangements throughout 2018. The IPC does not seek in any way to discourage 'non-RIPA' surveillance but instead public authorities should usually follow a RIPA-style approach in these circumstances."*[118]

The point that 'authorities need to be careful in these circumstances' is of particular importance given the intended removal of a legal duty to have regard to a formal code of practice published by the Home Secretary and the attendant independent oversight body that provides proactive guidance and consultation to surveillance operators (see Part Two). The application of approaches governing covert surveillance to overt activities is also highlighted in European case law. For example, in *Catt v. the United Kingdom* the European Court stated that case law addressing covert surveillance should guide other forms of surveillance, where,

> *"The powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology is continually becoming more sophisticated […] it should be guided by this approach especially where it has already highlighted concerns relating to the ambiguity of the state's powers."*[119]

While *Catt* addressed the retention of a protesters personal data gathered through overt surveillance it can be argued that to be equally applicable to police facial recognition deployments, particularly given the increasing capability of this technology and ambiguities over

[117] AB v Hampshire Constabulary Investigatory Powers Tribunal IPT/17/191/CH. Judgement available from https://investigatorypowerstribunal.org.uk/wp-content/uploads/2019/02/IPT-Judgment-AB-v-Hants-Constabulary.pdf

[118] Anthony Porter, former Surveillance Camera Commissioner, Futures paper provided to the authors.

[119] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 114.

its use. For example, in *Glukhin v Russia*,[120] the nature of a peaceful protest (similar to that in *Catt*) was transformed by the use of retrospective facial recognition technology to identify a protestor. Live facial recognition technology was then used to later locate and engage this individual.

Relatedly, paragraph 109 of *Bridges* cites the Government's SCCoP as a means of providing clarity, and thereby reducing arbitrariness, in such circumstances.[121] Also important to note is how paragraph 118 of the Court of Appeal ruling explicitly said that the *Code could be developed* to set out requirements for inclusion on a facial recognition watchlist, and how this national standard would be useful over diverging local policies governing use of this technology.[122] Expert interviewees for the report highlighted that many gaps left by this Bill could also be addressed if responsibility for the Government's SCCoP (updated only recently by Parliament) also moved under IPCO. This argument highlights how such a move would harmonise all functions for oversight of traditional and remote biometrics in policing under one established and internationally regarded judicial oversight body. Such a move could also add genuine 'future proofing' by anticipating the increasing potential for blurring boundaries between overt and covert surveillance brought by new advances in technology.

The preceding sections highlight the need for an agile form of oversight, one that can account for emerging technologies and associated practices. This further underscores the importance of the relationship between law and policy. As outlined in Part One, while law can set the overall direction in more abstract terms, policies are the means to implement such ambitions in a meaningful sense. Policies also have the agility to address emerging issues in a fast-moving operational context such as digital policing. As stated earlier, it is notable that this relationship was referenced to the 2020 *Bridges* Court of Appeal judgment, where the Government's SCCoP was cited as a means that could legitimate its use with the absence of an explicit legal framework.[123] Abolishing this Code, combined with the absence of any provision to replace it,[124] critically undermines this relationship.

With respect to live facial recognition technology, expert academic and practitioner opinion has been consistent in calling for *additional*, rather than reduced, codes to govern its use. Concerns have been raised over the lack of FRT oversight by the Mayor of London (GLA 2018) and the UN's Special Rapporteur for the Right to Privacy.[125] Additionally, both the House of Commons Science and Technology Committee[126] and the Equality and Human Rights Commission[127] have publicly called for a moratorium on uses of facial recognition technology in the absence of proper regulation. Echoing these sentiments, both the independent Ada Lovelace Institute review

[120] *Glukhin v. Russia* App no 11519/20 (ECtHR, 4 July 2023).
[121] *R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058].*
[122] Paragraph 120 of the same judgement also defines two 'critical defects in the current legal framework' as the absence of requirements "requirements as to the content of local police policies as to who can be put on a watchlist. Nor does it contain any guidance as to what local policies should contain as to where AFR can be deployed." The Court singles out the SCCoP as not containing requirements in these areas, which could be read as an argument to extend the Code.
[123] See, for example, paragraph 118.
[124] It is important to acknowledge the government's argument here that this Code represents a duplication of the ICO CCTV code. However, and as discussed in Part 3, this argument is rejected here on several grounds. The first is that the Government Surveillance Camera Code is widely regarded by surveillance camera users as an essential tool for maintaining standards in the profession and, accordingly, surveillance camera users are far more reliant on the SCC Code. Additionally, basic scrutiny of both codes reveals considerable differences that cannot be described meaningfully as "duplication".
[125] UN OHCHR (2018) *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland*, Geneva: UN OHCHR available from https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E
[126] House of Commons (2019) *House of Commons Science and Technology Committee: The work of the Biometrics Commissioner and the Forensic Science Regulator, Nineteenth Report of Session 2017–19*, London: House of Commons, available from https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf
[127] Equality and Human Rights Commission (2020) Facial recognition technology and predictive policing algorithms out-pacing the law, available from https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law

of biometric regulation[128] and the ICO[129] have called for the regulatory basis of such codes to be strengthened so they become legally binding with provisions for meaningful enforcement. This would avoid any prospect of 'cherry picking' from the proliferating guidance, ignoring that which exists but is not enforceable [130] and "*clarify the limitations on the use of [Live Facial Recognition] LFR, setting the required criteria for strict necessity and proportionality and required safeguards"*.[131]

The importance of this relationship between law and appropriate surveillance-focused policy applies more broadly. Such policies may also offer constructive resolution to different interpretations of the law and differences of opinion between surveillance users and oversight bodies. The following reflection from a senior police officer with national leadership of police ANPR surveillance illustrates these points,

> *"The one area we have had some disagreement with [the BSCC] on is the need for a specific legislative framework for ANPR. There's no primary legislation that governs how we are managing ANPR, unlike data communications. We are operating by interpreting other [relevant] legislation, the data protection legislation and what that means for ANPR. We have incorporated this into our NASPLE[132] guidance. The BSCC wishes to lobby the government for primary legislation to cover ANPR. I don't consider that pressing, saying "I think the existing legal framework and NASPLE, with the IAG initiative established with the SCC, works".[133]*

The above sets out the value of clear codes and policies to make broad 'principles-based' legislation focused, meaningful and implementable. Within this context, it is particularly notable that the Bill proposes to remove the duty on the Government to publish a SCCoP. Deleting legal instruments and attendant policy vehicles designed to operationalise broadly conceived principles-driven oversight legislation risks depleting the meaning and effectiveness of the latter. Academic research has evidenced how vagaries in regulatory frameworks impact users of advanced digital surveillance tools in complex ways. This includes the potential to deplete public safety through hesitancy in using legally permissible policing tools or, conversely, undermining rights protections through licentious interpretations of ill-defined regulation.[134] Moreover, the existing BSCC role is a means of offering forward leaning, expert focused and responsive engagement with surveillance users. This is complemented with a legally binding SCCoP established under a statutory framework that also confers credibility and status within practitioner communities.

Retrospective focus

A further rationale for retaining the Government SCCoP, and a recognisable surveillance-focused oversight structure around it, is because of the way law and policy has developed in this area. One of the reasons for the current complication of the regulatory landscape is because many developments, including POFA, arose as a response to a public, political or legal challenge to poorly regulated biometric or surveillance practices. For example, The Investigatory Powers Act 2016 was a direct response to the 2013 Snowden revelations detailing unregulated collection of communications data. The biometrics related provisions of POFA were a direct result of a European Court of Human Rights ruling on the unregulated retention of DNA data.[135] Erasing

---

[128] Ada Lovelace Institute (2022) *The Ryder Review*.
[129] ICO opinion October 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
[130] E.g. SCC (2020) *Facing the Camera* available https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf .
[131] Ada Lovelace Institute (2022) *The Ryder Review* recommendation 4.
[132] NASPLE: National ANPR Standards for Policing and Law Enforcement available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091167/NASPLE_Version_2.4_July_2022.pdf
[133] Interview with Chief Constable Charlie Hall, Hertfordshire Constabulary and National Police Chiefs' Council lead for ANPR
[134] See for example, Fussey, P., and Sandhu, A. (2022) 'Surveillance Arbitration in the Era of Digital Policing', *Theoretical Criminology*, 26(1): 3-22 Open Access available here.
[135] *S and Marper v United Kingdom* 30562/04 [2008] ECHR 1581

scant existing oversight frameworks – and without properly scoping out and anticipating emerging challenges – is likely to reproduce this cycle of retrospective action. It also challenges the credibility of claims that the new initiates are 'future proofed'. As the current BSCC stated in an interview, "*the landscape we've currently got now including is not the result of a Eureka policy moment. We've been sued here. We've been sued into shape.*"[136]

It can be argued that the complexity of the current approach has been driven by limitations on oversight that have given rise to legal challenges. As such, further removal of oversight is likely to reproduce this dynamic. The origins of this problem were also highlighted by all academic experts interviewed for this report,

> *"[biometrics oversight] was just a response to what had already been picked up historically, which is why it's got that random character to it. And that the UK Government historically has taken this very minimalist approach to responding to convention judgments. They literally look at the wording of it every full stop and comma, and don't look to the underlying principle. They just do a black letter law, transposition. And then, you know, you get this argument, oh, we're just trying to transfer in this is a way of not looking at some of the new techniques that are coming in."*[137]

Whilst principles-based approaches are a stated ambition of the Government, such principles are not clearly articulated in the Bill or its Explanatory Notes. The vehicle for delivering these principles are also unspecified or, as in the case of the SC Code of Practice, due to be abolished. Another academic expert similarly highlights the origin of a convoluted oversight picture and additionally emphasises how this is likely to re-emerge in the future,

> *"There are important functions that the biometric commissioner has that are laid down in statute for the very important reason that we got our beaten up the European Court [of Human Rights]. The DNA database was unlawful, it was breaching the Human Rights Convention. And in order to make it human rights compliant, we appointed a biometrics commissioner to oversee it… to get it in line they had to be dragged kicking and screaming…*
>
> *So, to make it anything like human rights compliant was to get a Biometrics Commissioner. So, all this stuff about national security determinations, of being able to retain biometrics if the police asked nicely. All of that was premised on there being an independent adjudicator with the power to say yes or no, who wasn't in the police and wasn't in government. And this is how we made our DNA database compliant with the Human Rights Act. So now, you can't just a few years later, then go, "oh, yeah, we've done that for a few years. Now, let's get back to where it was before…*
>
> *We keep relearning the same lessons and having the same arguments over and over again. Why can't we just say, "look, we already learned this lesson from the DNA database, you just don't give the police carte blanche to do whatever they want, with deeply personal biometric information because you'll get in trouble". Otherwise, we'll have to claw our way back again, and try and reverse engineer it… If we just took an informed view of new biometrics, such as facial recognition, and step away, we are going to have to mount these arguments again. Because if they take away that oversight, they will lose legitimacy. And if you don't have legitimacy, then people will start poking holes and ask if any of this actually lawful. And then we have to get through the courts again. And then you'll have to have the police in the home office defending this debacle and stuff… what are they doing with police uses of all that dashcam and doorbell footage?"*[138]

This point was also highlighted by the current BSCC who highlights the diversification of surveillance capabilities and the changing role of video footage in investigations,

[136] Interview with the Biometrics and Surveillance Camera Commissioner.
[137] Interview with Professor Lorna Woods
[138] Interview with Professor Carole McCartney

> *"I think both technologically and societally there is an enormous expansion in both capability for public space surveillance, and concern about it. So whatever it looks like today, this will look really easy in five years time. And in order to address both of those, the burgeoning capability, if we're going to harness it properly, and also to assuage at the same time legitimate public concerns… I mean, when you go back to that, you look at the fact that DNA contributes to 1% of police investigations in the UK. And look at how we regulate it. And yet, if we have probably 70% of investigations that rely on social media and citizen shared data at the moment. Dashcam, ring doorbell, GoPro footage. Either people send it in voluntarily or it's in response to an appeal. And that's totally unregulated. And in the future, it's only going to grow…*
>
> *We will grow enormously in terms of public space surveillance data, whether it's official or unofficial. And so shouldn't we have a regulatory framework that reflects the relative contribution to investigation? Yes."*[139]

Another expert participant questioned the degree to which the Bill can be seen as future proofed given the lack of specificity. He also located the approach in a more enduring trend over the governance of police technologies,

> *"The Bill doesn't seem future proof in my mind… I've yet to see the Government lift a finger to anticipate the legislative frameworks and codes of practice that would be required for the emergence of new police technologies before the technology is deployed. We have an ad hoc police "do your own thing" arrangement, and if there's anything to challenge, the courts can mop it up, and we will do something with the consequences. Usually the bare minimum. I think that's a pattern that is played out famously [with] DNA retention and the protracted human rights challenge in S and Marper v the UK followed by a sort of piecemeal legislative intervention to address the human rights judgment. A similar thing happened with the custody images, there was a High Court challenge to retaining any and all custody images of arrestees regardless of conviction. So then, the Home Office conducts a review, following an adverse judgement [in R(RMC and FJ) v CPM [2012] EWHC 1681], and does some tinkering at the margins. You can now write to have the custody image removed. which no one ever does because they don't know they're entitled to do that. A similar trend in criminal records disclosure cases. Another example is facial recognition. What we have is adoption and use of surveillance technologies by the police, a slow process of challenge and review of that use on narrow terms - because judicial review is not designed to provide wide regulation of police use of technologies - and then minimalistic legislative reaction born out of being legally mandated to react the addresses the issue narrow grounds on which the review was argued. Basically, we're quick to use these technologies very slow to develop regulation. That's been the tradition and this bill might continue that trend".*[140]

The above stresses the need for vehicles to deliver focused policies while holding the agility to address emerging issues. Moreover, designated surveillance-focused expertise and an ability to engage with the public and range of stakeholders, such as that encompassed by the BSCC role, is deemed vital in securing public confidence in the use of biometric materials.

Coverage

Excluding IPCO, expert interviewees questioned the suitability of alternative venues for surveillance and biometric oversight. The Government position is that most prominent venue for the continuation of these oversight functions is the UK data protection authority, the Information Commissioner's Office (ICO), and under the provisions in the Bill the newly formed Information Commission. One of the central issues affecting the role of police and local authority surveillance oversight being subsumed into the remit of a data protection controller is that the ICO and BSCC offer different forms of oversight and focus on different challenges. These are addressed in turn.

[139] Interview with the Biometrics and Surveillance Camera Commissioner
[140] Interview with Dr Joe Purshouse.

Different forms of regulation

As pointed out by a former Biometrics Commissioner in his (unpublished) response to the consultation, "*neither the Camera Commissioner nor the UK Biometrics Commissioner are 'regulators": they have no regulatory inspection powers nor any enforcement powers to ensure compliance with the requirements of PoFA"*. The current BSCC also pointed out these differences in his response to the same consultation, *"[t]o propose absorption of the Biometrics and Surveillance Camera Commissioner functions by the ICO is to misunderstand the realities of those functions".*

Instead of 'harder regulation', and as detailed in Part Two above, the BSCC uses a range 'soft levers' to ensure compliance and to raise standards. These include annual reporting, proactive engagement with both biometrics and surveillance practitioners, encouragement to adhere to the code of practice and other mechanisms, such as the certification scheme. This differs from the approach and constitution of the Information Commissioner as a regulator, holding statutory powers to request information, conduct inspections and determine actions and penalties. In a former Biometrics Commissioner's estimation, the ICO is "*one of the most powerful regulators in the UK*".[141] How far replacing this role with a corporate regulator as proposed by the Bill will affect that situation remains to be seen.

An argument exists that the harder regulatory model provided by the ICO would raise the overall level of oversight and offer more protections against breaches. However, this position is caveated by several factors. This includes the effectiveness of the POFA model in encouraging surveillance users to raise standards and, separately, the limits to data protection as a means to address the range of surveillance-related impacts on the public. These are discussed in turn.

Engagement

Government documentation argues that "*current oversight arrangements for police use of biometrics and surveillance cameras to help identify and eliminate suspects are complex and confusing for the police.*"[142] Academic research reveals that perspectives of oversight and regulation are varied within law enforcement communities. One Chief Constable holding national leadership for ANPR surveillance describes the benefits of the current arrangements,

> *"The Surveillance Camera Commissioner has helped hold our feet a little bit to the fire around that I guess. It's felt, it's felt easier to do it that way than it would be if it was through the ICO as they're a regulator. So you can have a bit of a different conversation, I think, sometimes, with the Biometric and Surveillance Camera Commissioner… those initial discussions were easier to have. [we could ask] what do you think? Are we being reasonable? Or are we not around this?"*[143]

The value of such proactive conversations for the opportunity to embed good practice from the outset was echoed strongly across law enforcement contributors to this report. For example, a Deputy Chief Constable with national leadership for police Body-Worn Video stated,

> *"The beauty about Fraser's office was that he proactively leaned in, in a supportive way. You know, I didn't have to go looking for Fraser. Fraser came to me and said, "look, can we have a conversation? I just want to understand where you're going with the portfolio. These are some perspectives I want to share with you". Whether it was his own personal style, or whether it's the way the office is structured, he had the capacity and capability to proactively lean into law enforcement in a way that I've not seen any other agency or regulator seek to do".*[144]

[141] Prof Paul Wiles, Commissioner for the Retention and Use of Biometric Material by the Police 2016-2020, unpublished submission to the original consultation supplied to the authors, reproduced with his kind permission.
[142] DPDI Bill Explanatory Notes p.13
[143] Interview with Chief Constable Charlie Hall, Hertfordshire Constabulary and National Police Chiefs' Council lead for ANPR.
[144] Interview with Deputy Chief Constable Jim Colwell, Devon and Cornwall Police. National Police Chiefs' Council lead for Body Worn Video.

An academic expert offers a similar point, seeing the "*ICO as it stands now, is, it seems to me, a highly reactive body*". While a key point here that such assessments are made on how the ICO currently stands, the Bill provides no detail on what a reconstituted ICO would look like.

Moreover, while the ICO hold powers of inspection that are not endowed to the POFA commissioners, such inspections take place on different grounds and for different purposes. However, this would not be a primary focus of their work and such inspections would take a different a character compared to the BSCC certification schemes.

Much of this variation arises from the difference between 'data protection' and 'surveillance'. While overlap clearly exists (such as in the use of data generated in the course of surveillance operations), the differences are significant. These differences are crucial when considering the claim that OBSCC work duplicates that of the ICO.

Differences between data protection and surveillance

While overlaps between oversight provided by the BSCC and Information Commissioner are discernible several important differences exist.

A starting point is to consider how other forms of surveillance deemed intrusive have been facilitated through an explicit legal basis accompanied by a legally enforceable regulatory framework. For example, and taking the argument to a logical conclusion, if potentially intrusive surveillance tools could be effectively governed through a data protection regime it would question why other forms of surveillance were considered necessary to require additional oversight to ensure compliance with human rights obligations, as demonstrated in the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016. Moreover, given a Data Protection Act was in force for 27 years before the Biometrics and Surveillance Camera Commissioners were established under POFA, questions are raised over why the latter was deemed necessary in 2012 (discussed below). While many of the above interventions cover intrusive forms of covert surveillance, they demonstrate, categorically, that potential surveillance harms extend beyond issues of data protection.

This issue has several components. The first covers the exceptionality of law enforcement activities, something recognised in other regulatory approaches.[145] As stated in the BSCC response to the original (DCMS) consultation,

> *"while they involve oversight of the lawful processing (including retention and sharing) of some highly sensitive personal data, the functions of the Biometrics and Surveillance Camera Commissioner go far beyond data protection'. As noted by both the United Nations and Interpol, law enforcement is an 'information-based activity' and what often differentiates the police from other bodies is the purposes for which they need to use information, purposes which necessitate the collection, retention, sharing and deletion of biometric material and surveillance images."*[146]

This is because, in order to fulfil their functions, "*law enforcement activities often involve tools, tactics and techniques that are deliberately and necessarily intrusive, with some representing a significant and enduring interference with the citizen's basic human rights*".[147]

The issue of law enforcement highlights an important difference between the work of data protection regulation and the work of the BSCC. The Scottish Biometrics Commissioner considers it important to differentiate between data protection and criminal procedure,

---

[145] For example, the EU Law Enforcement Directive that companions the EU GDPR.
[146] OBSCC response to the consultation, available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1030248/BSCC_DCMS_Consultation_Response.pdf
[147] *Ibid.*

> *"Now, the ICO, as you know, is interested in upholding the Data Protection Act, and that pulled in people's information rights. But, now, it isn't interested in upholding Criminal Procedure Law. The statutory functions of the ICO do not extend to questions of effectiveness or efficiency in relation to the police use of biometric data. They're not interested in ethical considerations of that. And, I mean, you can see that a good example, if you think of the Marper[148] case from 2008, that ruled the police were holding lots of data illegally. And all these years later, they still are because nobody has done anything to prevent them from, from doing it."*

Professor Lorna Woods, a Professor of Internet Law, elaborates on these differences,

> *"Often surveillance technologies can operate in such a way that they may not raise significant or serious data protection concerns…*
>
> *I suppose it's a caricature and sort of overstates the difference, to help explain it, but data protection is about how data processing happens. It's sort of saying if you've got a legal basis, it's okay. It doesn't really look into the acceptability of the purposes. I mean [considerations of] legitimate interest [exist that] you have to balance against it, such as privacy. But, fundamentally, it's value neutral. In that sense, you could be using [data] to discriminate, to plan a euthanasia campaign, you know. It has some consideration but it certainly doesn't really fully engage with power relationships. I hesitate saying that, because obviously, there's the constraints on when, when consent happens…*
>
> *Whereas surveillance is recognising that the state has power. And that it in using that power on all citizens there is a risk that that power can get abused. When you're talking surveillance, you have to justify why you're doing it in a way you don't when you're talking about data protection, data protection is. Have you got the legal basis? Is it within the purposes you've collected it for et cetera. Whereas an analysis on surveillance, and you're drifting much more into rights territory, when you're talking about surveillance, because it is that core of the negative obligation on the state not to interfere with private life. You really just define in the public interest, not just any interest."*[149]

A former Surveillance Camera Commissioner highlighted how 'surveillance material', the product derived from a surveillance camera, can serve multiple roles and may be constituted as 'personal data', but also evidence, intelligence and information. He additionally pointed to the *RIPA Code of Practice for Covert Surveillance and Property Interference*[150] as an example of how 'surveillance conduct' undertaken by state actors may engage a broader range of statutory and regulatory considerations beyond data protection.

One senior police officer serving as the National Capabilities Manager for CCTV also highlighted differences between surveillance material and personal data,

> *"Everyone in the [United] States that gets arrested or put in prison now have their Iris, photographed. Biometrically. It's about the standards behind that, making sure that it's done appropriately. And obviously, the data stored correctly. But also the technology around that. Because we're still having problems in UK policing with the quality of our custody images. You know, we'd spent a long time producing the facial images, national database standards, not all forces were in a position to implement those standards. So when you look at the quality of images across the board that are going into the police national database, there's a huge difference. And this is where the biometrics side really supports where we are with that tech."*[151]

---

[148] *S and Marper v United Kingdom* 30562/04 [2008] ECHR 1581
[149] Interview with Professor Lorna Woods.
[150] See, for example, *RIPA Code of Practice for Covert Surveillance and Property Interference*, section nine, pages 73-88.
[151] Interview with Andy Read, South Wales Police, National Police Chiefs' Council National Capabilities Manager for CCTV

Notable here is how decisions over surveillance activities that may sit outside data protection law may generate implications for data protection governance. This suggests considerations of issues that fall outside of data protection law, such as those undertaken but the BSCC, may uphold higher data protection standards in the long run.

The cumulative impact of coalescing such wide-ranging functions into a data protection regime may therefore reduce the quality of data protection activity itself. This issue is summarised by one surveillance law expert as an overall depletion of oversight,

> *"Pulling oversight away from a Surveillance Camera Commissioner, whose role is to consider broad social impacts, for better or worse, of particular camera-based public surveillance technologies, and to take account of different legal frameworks that bite upon the use of facial recognition technology? And to put that into the remit of the Information Commissioner's office? It seems to me that you will lose expertise, and layers of oversight, accountability and forward-looking guidance and perspective. It could have an effect of making surveillance oversight and regulation quite reductive".*[152]

Forms of data

Cutting across many of these accounts is the classification of information that falls under the jurisdiction of a data protection controller such as the ICO, and that which falls outside. As one academic expert on surveillance oversight explains,

> *"an example might be something like mass data retention or something like that. The data that's taken, aggregated and processed may not actually involve analysing personally identifiable information. The information might all be deidentified. The consequences of collecting and processing that data and that information on a mass scale can be quite severe for people's freedoms, their democratic rights, their abilities to organize online, the balance of power between the States and the individual, for those harms may not be captured at all through a data protection lens".*[153]

In developing this discussion, the Forensic Science Regulator makes an important clarifications and distinctions around biometrics and forensic 'applications' and, these considerations complicate the idea that biometric applications and materials are reducible to issues of data protection,

> *"I would like to comment on the differences between what I would refer to as a biometric and forensic applications. As you will see from my comments this is not a clear distinction. In simple terms a biometric application could be considered as identity validation in that the material or information being used is taken under control conditions is of high definition or discriminating power and amenable to automated comparison with a high degree of accuracy with limited human intervention, the use of passport images is an obvious example of this. In a forensic application while sometimes there may be a need for identity validation the vast majority is based on the recovery of material in uncontrolled situations where the data may be degraded or limited and a comparison can only give a limited connection between the recovered unknown or reference material, an example would be the recovery of DNA information that is only a partial match with the reference material there is the potential that many people share the same DNA information and that of the recovered material. I have no expertise in privacy or data protection but in a forensic context the determination of what is personal data in that it can be attributed to an individual is not a straightforward issue. There are different considerations for fingerprints, DNA and face and in view of the changes anticipated and the abolition of the Office of the Biometrics and Surveillance Camera Commissioner role I have opened up a dialogue with the ICO so that we have a joined up view of the regulation of forensic and biometric data, the views of the Biometrics and Surveillance Camera Commissioner would have been an important contribution to this discussion."*[154]

[152] Interview with Dr Joe Purshouse
[153] Interview with Dr Joe Purshouse
[154] Written submission from the Forensic Science Regulator

A similar point is made by the Biometrics and Surveillance Camera Commissioner in his submission to the original Bill consultation,

> *"The police use of biometric data in the making of National Security Determinations, counter-terrorism policing and prevention [of] serious crime could be characterised as 'data protection' in the same way as their use of facial recognition cameras could be characterised as 'photography'. It is the potential interference with fundamental human rights presented by law enforcement activities which calls for very specific safeguards, accountability mechanisms and governance frameworks going beyond compliance with basic data protection principles."*[155]

A related point is offered in a recent expert-led review of biometric regulation, arguing that the *classification* of biometric data does not necessarily constitute *identification* and thus personal data, yet may generate similar degrees of intrusion.[156] This equivalencing of harm as it applies to identification and classification has been rejected by the Government, as stated in the response given by Sir John Whittingdale, Minister for Data and Digital Infrastructure, that "using biometric data to draw inferences about people, using algorithms or otherwise, is not as *invasive* as using biometric data uniquely to identify someone".[157] Such statements represent a narrow view of harms in terms of 'invasiveness' and necessarily downplays the long established, documented, impacts of data categorisation on people.[158] Even if the Government argument of a lesser degree of invasiveness were to be accepted, thew fact that such activities remain invasive implicates a need for oversight.

Limits to data protection approaches when dealing with aggregated data for surveillance purposes was also raised in the BSCC's submission to the original Bill consultation,

> *"Moreover, whereas new technology can enable greater specificity, 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."*[159]

These concerns are made more acute by the proposed narrowing of the definition of 'personal data' under the DPDI Bill. Clause 1(2)[160] of the Bill changes the threshold for personal data as,

> *"Information relating to an identifiable living individual only in cases … where the living individual is identifiable by the controller or processor by reasonable means at the time of the processing… where the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing, and… the living individual will be, or is likely to be, identifiable… by that person by reasonable means at the time of the processing (emphasis added)."*

This reference to 'reasonable means' focuses on the capacity of data controllers to foresee identifiability.[161] In addition, and while not exclusively so, heavy emphasis is placed on the point

---

[155] BSCC response to the consultation, available here: https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version

[156] Ada Lovelace Institute (2022) *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, P71-72 available from https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

[157] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf p.276. Emphasis added.

[158] E.g. inter alia Lyon 2003, Graham, 2005, O neill 2016, Eubanks 2017 Zuboff 2019.

[159] BSCC response to the consultation, available here: https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version.

[160] Clause number unchanged across all versions of the Bill.

[161] Subsection six of this clause elaborates on the criteria for "whether a person is reasonably likely to use a means of identifying an individual". The Bill states that this

of collection. The result is a narrower definition of what constitutes 'personal data' and the increased likelihood that the 'surveillance material' discussed above falls outside this category. As one recent briefing from a civil society group argues,

> *"Changing the definition of personal data in this way allows more data to be processed with lower levels of protection, narrowing the scope of information safeguarded by data protection law and placing disproportionate power in the hands of the data controller. In practical terms, businesses will be able to process more data than they are currently permitted. This is determined by a wholly subjective test that is measured by a business's capacity and context "at the time of processing."*[162]

The briefing then considers the impact of such classifications on facial recognition surveillance,

> *"Data protection expert Dr Chris Pounder explains how this could increase data processing with minimal safeguards in the context of facial recognition CCTV, as the threshold for personal data would only be met if the data subject is on a watch-list and therefore identified. If an individual is not on a watchlist and the camera images are deleted instantly after checking the watchlist, then the data may not be considered personal and therefore would not qualify for data protection obligations. This would put the UK completely out of step with the rest of Europe."*[163]

Rather than simplifying oversight, this would also bring the UK out of step with its own judicial rulings on facial recognition technology. The Divisional Court in the *Bridges* Judicial Review ruled that an individual's personal data is processed by facial recognition cameras irrespective of whether they were enrolled onto a watchlist, on the grounds that the technology causes people to be 'individuated' from others.[164, 165]

These proposed changes mark a clear depletion in the oversight of surveillance measures such as facial recognition. Individual rights that, in the recent opinion of the Divisional Court, were engaged by virtue of being scanned by FRT, are to be considered irrelevant under the current formulation of the Bill. As such, not only is surveillance oversight depleted through its incorporation into generic data protection regulation, data protection regulation itself becomes depleted under the arrangements of the Bill.

Range of Rights

The Bill makes it clear that the ICO would be reconstituted into a new "Information Commission" that incorporates a full transfer of the functions of the Information Commissioner. The Guidance notes accompanying the Bill state that 'the nature of the regulator's role and responsibilities remains unchanged'.[166] It is therefore reasonable to assume the existing ICO approach to data protection would apply across the oversight of public surveillance.

"is to be determined taking into account, among other things—

(a) the time, effort and costs involved in identifying the individual by that means, and

(b) the technology and other resources available to the person."

Therefore, the size of an organisation conducting the processing dictates the level of protections offered to the individual who's data is to be processed. According to one anonymous contributor to this report, this shifts the emphasis from the 'nature of the data to the nature of the controller'.

[162] Big Brother Watch (2023) Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Committee Stage, p.9. Available from https://bills.parliament.uk/publications/51054/documents/3385

[163] Ibid. p10

[164] R *(on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058]* para 46. Also see: https://amberhawk.typepad.com/amberhawk/2023/04/facial-recognition-cctv-excluded-from-new-data-protection-law-by-definition-of-personal-data.html

[165] Chris Pounder also makes this point in a blog post supporting his submission to the Commons Committee. The blog post is available here: https://amberhawk.typepad.com/amberhawk/2023/03/dpdi-no-2-bill-should-be-paused-until-the-uk-bill-of-rights-position-is-resolved.html and the Committee submission here: https://bills.parliament.uk/publications/51049/documents/3383

[166] DPDI Bill Explanatory Notes paragraph 643, p.85

It has been widely acknowledged that, while important elements of the overall picture, potential harms of surveillance extend beyond issues of data protection and privacy.[167] This generates issues concerning the degree to which the range of fundamental rights are protected when surveillance oversight is placed under a data protection regulation regime.

This applies in a general sense and with respect to discrete forms of biometrics and surveillance. Regarding the former, many participants including the current BSCC and a former Surveillance Camera Commissioner questioned the scope of the Data Protection Act in addressing surveillance oversight,

> *"The Data Protection Act 2018 does not provide a sufficient basis in law for the conduct of surveillance by means of overt surveillance camera systems such as ANPR and AFR in the same manner that RIPA does in terms of covert surveillance".*[168]

The former Surveillance Camera Commissioner also noted that this was an opinion echoed by the Information Commissioner's QC at the high court case on AFR in 2019.[169]

One academic expert detailed the limitations of data protection approaches to addressing facial recognition technology,

> *"A technology like facial recognition has impacts that are broad and diverse. They can't be captured through reference to any sort of discrete area of harm, such as, for example, data protection law, which is an oversight mechanism designed to ensure that people's personally identifiable data isn't misused. Public surveillance measures have consequences that extend beyond this, such as the right to as assemble and participate in democratic process processes, protests, and dissent. They can have discriminatory potential and equality based concerns. When looking at a regulatory frameworks to guide the police on the appropriate limits of any experimentation with new sector surveillance technologies such as facial recognition you need to have oversight that takes this broader view of potential harms, is capable of doing that, and is institutionally competent to who take account of these broader surveillance impacts."*[170]

The BSCC's submission to the original consultation makes a similar point,

> *"Not all considerations arising from the police use of biometrics and surveillance cameras are data protection issues. An example is the potential for the presence – or even the perceived presence – of a police surveillance camera to discourage people from meeting, from expressing views or exercising their right to protest peacefully. As one research study involving the US Department for Homeland Security and the Federal Bureau of Investigation conceded "The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behaviour, and lead to self-censorship and inhibition."*[171]

Such 'chilling effects' of surveillance have been documented extensively.[172] While acknowledging the relationship between privacy and other fundamental rights is complex, the impact of chilling

---

[167] Murray, D. and Fussey, P., (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. Israel Law Review. 52 (1), 31-60

[168] Interview with Anthony Porter, former Surveillance Camera Commissioner.

[169] Interview with Anthony Porter, former Surveillance Camera Commissioner. The case referred to is *R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341 (Admin)*, the original (rejected) High Court application for Judicial Review on uses of facial recognition technology..

[170] Interview with Dr Joe Purshouse.

[171] OBSCC response to the consultation, available here: https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/dcms-consultation-data-a-new-direction-response-by-the-biometrics-and-surveillance-camera-commissioner-accessible-version

[172] E.g. Canes-Wrone B and Dorf M (2015) Measuring the Chilling Effect. *New York University Law Review* 90: 1095–1114; Kendrick L (2013) Speech, Intent, and the Chilling Effect. *William & Mary Law Review* 54(5): 1633–1691; Manokha I (2018) Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society* 16(2): 219–237; Marthews A and Tucker C (2014) Government Surveillance and Internet Search Behavior. *MIT Sloane Working Paper No. 14380*; Penney JW (2016) Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal* 31(1): 117–182; Solove D (2007) The First Amendment as Criminal Procedure. *New York University Law Review* 82: 112–176; Stevens, A., Fussey, P., Murray, D., Hove, K. and Saki, O., (2023). 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in

effects of surveillance is often associated with the rights to freedom of expression, and the right to freedom of assembly. The outcome is an impact that exerts itself on the human rights essential to the development of personal identity and, by recognising the links between expression and assembly, that surveillance impacts are not only a matter of individual privacy or individual expression, but also directly impact at a societal level, particularly on democratic processes.

One relevant example is the use of live facial recognition in public places. The London Police Ethics Panel report into Metropolitan Police uses of this technology evidences opinions of Londoners that states 38% of those aged 16-24 agreed with the statement "I would stay away from events where I know LFR would be used".[173] The scale of such concern suggests the need for an oversight mechanism to affect these specific affected rights.

The other significant area of debate concerns bias and its connection to the fundamental human right of the prohibition of discrimination (Article 14 of the European Convention on Human Rights) and the Public Sector Equality Duty under the Equality Act 2010. Much has been written on the biases that may be inherent in emerging surveillance technologies, particularly facial recognition. This debate is complex and is too voluminous to rehearse in detail here. However, that FRT capability varies across different demographic characteristics is an established scientific fact. The most authoritative and comprehensive research into this issue to date tested 189 commercially available face recognition algorithms from 99 separate suppliers on a bank over 18.27 million images of 8.49 million people to conclude that all facial recognition algorithms performed unevenly across different demographic groups (NIST 2019). FRT treats people differently depending on their demographic location. Other research that has been used to suggest an absence of demographic bias (e.g. NPL 2023)[174] also highlights inherent biases in the algorithm.

Several sources have pointed out that because data protection is focused on personal data, it is a less equipped to address group-level harms. This was expressed in the recent Ryder Review of UK biometrics,

> *"This is in part because data protection laws focus on 'individual (rather than group) conceptions of harm [which] fails to meaningfully address questions of discrimination and algorithmic profiling.' This was also a concern we heard from Big Brother Watch, particularly when discussing the Bridges judgment. The use of existing sources of law, both data protection and human rights law, as the entry point for biometric governance, fails to take into account some of the specific features and specific risks posed by biometrics, particularly on the group level."*[175]

A related issue concerns the proactive engagement with these issues to enhance legitimacy and trust in surveillance practices and policing more generally. The Deputy Mayor for Policing and Crime (DMPC) for West Yorkshire considers the requirements for a data protection regulator to address these issues,

> *"From the perspective as a Deputy Mayor, for [Police and Crime Commissioner], how would they [the data protection authority] know that that was a new function that they were undertaking? So there needs to be a big campaign around that. There needs to be a lot of engagement reaching into communities, which costs*

Zimbabwe. *Big Data and Society*. 10 (1); Stoycheff E (2016) Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly* 93(2): 296–311 ; Stoycheff E, Liu J, Xu K, et al. (2018) Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society* 21(3): 602–619; Murray, D., Fussey, P., Hove, K., Wairagala, W., Kimumwe, P., Saki, O., and Stevens, A. (2023) 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe' *Journal of Human Rights Practice*, Oxford University Press. Online first available here: https://doi.org/10.1093/jhuman/huad020

[173] LPEP report p24.

[174] Contrary to some reporting on this issue, the NPL report identifies inherent ethnic bias in facial recognition algorithms used by the police. The report argues that such biases are reduced to a level where they are 'not statistically significant' if the sensitivity of the system is significantly reduced (in a way that would also restrict the number of overall matches).

[175] Ada Lovelace Institute (2022) *The Ryder Review.*

> *money, so you've got to have the resources to do that. But they could only do it if they were given a different structure, more resources. And that was, you know, part and parcel of their work. They would need proper terms of reference and then campaign so that members of the public and other interested stakeholders knew their role."*[176]

Enforcement

Another consideration affecting the role of data protection authorities (of which the ICO is the UK's version) in surveillance oversight is that of enforcement. One argument is the Information Commissioner holds stronger regulatory powers than the BSCC and could therefore exert a more robust form of oversight. However, this argument is subject to two significant caveats.

The first is that, for understandable reasons, the ICO have developed an approach that is resistant to fining public bodies.[177] This is highlighted in the main ICO strategic plan.[178] It is also important to note an underreported aspect of ICO work, that of pro-active engagement to raise standards rather than solely working as a reactive regulator,[179] an approach the BSCC has received credit for (see above). However, the lack of formal enforcement against public bodies undermines the argument that DPA regulation is necessarily more punitive.

The second consideration is that, in an international context, data protection authorities have an extremely limited track record in investigating surveillance-related breaches. According to a 2021 analysis by IVPM, data protection authorities in the majority of GDPR countries (18 of 30) had issued either zero or only one video surveillance fine since the adoption of the GDPR in 2016 (and its enforcement since 2018). 14 countries, including the UK, had issued no fines.[180] This outcome brings complexity to the public Ministerial position that "The ICO will continue to provide independent regulation of the use of surveillance camera systems by all organisations".[181] The types of fines issued also reveal the focus of enforcement activities. Principal violations included unauthorised filming of public areas, insufficient signage, and illegally monitoring employees. Such findings suggest more evidence is needed to justify the effectiveness of data protection authorities in the regulation of surveillance.

ICO and Government Surveillance Camera Code of Practice for video surveillance

As stated above, the guidance notes for the Bill justifies the proposal to abolish the role of the Surveillance Camera Commissioner on the grounds that the role duplicates oversight of overt surveillance already provided by the ICO. The Bill explicitly proposes the deletion of the Surveillance Camera Code and related provisions on the grounds it is duplicated (see above) have been repeatedly expressed in public forums.

The key stakeholders interviewed for this report disagree that the Government Code represents a duplication of guidance offered by the ICO. *The* principal difference is that the SCCoP is a legal instrument published by the Government. By contrast, the ICO has no statutory obligation to produce a code. This issue also raises a further question over the issue of 'duplication'. The ICO would need to build capacity and acquire a new statutory duty in order to offer the same

---

[176] Interview with Deputy Mayor (Police and Crime) West Yorkshire

[177] Although the ICO asserts it reserves the right to do so in 'egregious cases', and commits to continuing the same level of investigation, regardless of whether an organization is privately or publicly funded. See https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/

[178] https://ico.org.uk/media/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan-0-0.pdf p.27

[179] One author also witnessed this approach in his independent review of the Metropolitan Police Service's test deployments of facial recognition in 2019 (Fussey and Murray 2019). The intention to proactively engage and offer advice is also stated in the main ICO strategic plan https://ico.org.uk/media/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan-0-0.pdf

[180] Two counter arguments should be presented here in the interest of balance. First, as mentioned above, the ICO tends to avoid fining public bodies, so the absence of fines does not automatically translate into the absence of investigations. Second, and relatedly, is the timeframe of the IVPM report, which focuses on the period since the GDPR (post 2016). One particularly high profile ICO investigation into surveillance occurred three years prior to this with the ruling that Hertfordshire Constabulary had broken the law with their extensive ANPR system encircling the small town of Royston (population 15,781) (see BBC 2013: https://www.bbc.com/news/technology-23433138)

[181] https://hansard.parliament.uk/commons/2023-05-23/debates/8a27fce9-285d-4e1b-8c1e-662f3600d681/DataProtectionAndDigitalInformation(No2)Bill(EighthSitting) Column 272

oversight as that currently offered by the OBSCC. Given the above, and aside from a superficial resemblance in the titles of both the ICO and Government codes, it is difficult to substantiate claims that the Government Code duplicates that published by the ICO. Basic scrutiny of both reveals the focus, adoption, legal constitution and purpose are palpably different.

An additional element is the law enforcement perspective. Rather than expressing confusion, all participants holding senior police roles, mostly involving leadership of national portfolios, were emphatic in their support for the SCC role and Government SCCoP. Moreover, when asked directly, many police representatives considered the Government SCCoP most relevant to their work. As one senior officer holding a national CCTV governance role stated,

> *"we are way, way more weighted towards the Surveillance Camera Code. In fact, I would suggest that's been in the background and driving a fair bit of activity, not necessarily directly, but indirectly."*[182]

Another senior officer stated that,

> *"The ICO are concerned with the output from this industry. You know, when you look at the civil liberties side of it, regardless of the fact that we're producing video footage of people walking down the street, it's actually the whole process of being able to create that information in the first place… It's the issue that we've actually got people sat there physically watching these other people walking around going about their business. And that's what we really have to control very securely because, obviously, within policing, we have to have directed surveillance authorities and other authorities with regards to being able to look at somebody. But the control over the operators and local authority systems etc., and the CCTV consultants that needed to be really well controlled."*[183]

Of note here is the way law enforcement participants stress stronger engagement with the Government's Surveillance Camera Code of Practice than the ICO guidance. The Deputy Mayor for Policing and Crime for West Yorkshire was particularly forthright in this view,

> *"I think the police don't think about the ICO from day one… police. I've been involved in policing governance for over 20 years. I can't remember once a Chief Constable or any of their command team talking about GDPR or conversations with the ICO."*[184]

Another nuanced view of this is offered by a Deputy Chief Constable with a national (NPCC) leadership role covering police body worn video. While the ICO were deemed important to overall responsibilities associated with being Deputy Chief Constable, the ICO were less prominent in work that specifically focused on video surveillance,

> *"My office has had more dealings with the ICO in my role as Deputy Chief Constable of a police force than as a national leader on body worn video. In fact, I think I'm yet to have any dealings with the ICO from a national portfolio perspective [covering body worn video]."* [185]

This limited engagement on video surveillance-specific issues was reflected by other senior officers holding national surveillance roles,

> *"We haven't had any good engagement with the Information Commissioner's Office for two years, they've essentially pulled out from any of our meetings. They said that we don't have the staff and a lot of the things that we're discussing isn't around data protection."*[186]

[182] Interview with Andy Read, South Wales Police, National Police Chiefs' Council National Capabilities Manager for CCTV
[183] Interview with Assistant Chief Constable Jenny Gilmer, South Wales Police, National Police Chiefs' Council lead for CCTV
[184] Interview with DMPC West Yorkshire.
[185] Interview with Deputy Chief Constable Jim Colwell, Devon and Cornwall Police. National Police Chiefs' Council lead for Body Worn Video.
[186] Interview with Andy Read, South Wales Police, National Police Chiefs' Council National Capabilities Manager for CCTV

Another senior officer underscores the complexity of this landscape and hence the value of simplification. Of note is how, in this crowded space, it is the Government's SCCoP that has the greatest influence on law enforcement practices. As one Chief Constable explains,

> *We will certainly work with the ICO and do already. But the development of ANPR oversight has been done in conjunction with what was the Surveillance Camera Commissioner. It mostly came to fruition in Tony's [the previous Surveillance Camera Commissioner] role when he agreed to convene and chair the IAG."*[187]

All law enforcement participants also stressed the strength of an existing positive relationship with the BSCC. Added to this was the sense that the BSCC had specific and focused expertise that could support policing. This was further expressed by another senior law enforcement figure holding a national strategic role covering overt surveillance,

> *"Whilst we are very respectful to the parameters of the role of the Commissioner, I think we've been fortunate with both Tony and Fraser [the previous and current SCC/BSCC postholders]. Informed individuals who "get it" and understand the journey that we're on. We're absolutely on our "turn the tanker" journey in relation to CCTV. I guess I would worry that we would become almost like at the mercy of a body that doesn't fully understand the challenges we're working with, and how much work is underway to address those."* [188]

Other oversight venues

As discussed above, the spectrum of potential surveillance harms transcends data-related matters. In response to this, the public Ministerial position is that several other venues exist to address these wider issues. As the Minister for Data and Digital Infrastructure, Sir John Whittingdale, argued at the Public Bill Committee stage,

> *"I point out that there is a comprehensive legal framework outside the Surveillance Camera Code. That includes not only data protection, but equality and human rights law, to which the code cross-refers. The ICO and the Equality and Human Rights Commission will continue to regulate such activities. There are other oversight bodies for policing, including the Independent Office for Police Conduct and His Majesty's inspectorate of constabulary (sic), as well as the College of Policing, which provide national guidance and training (emphasis added)."*[189]

This response namechecks various organisations that have varying degrees of relevance to biometric and public surveillance practices. However, it is incorrect to claim they provide any collective form of regulation in this space. For example, among those listed, only the ICO can be accurately described as a regulator. The limits of ICO regulation of biometric and public surveillance are discussed in detail above.

An important distinction here concerns the difference between inspectorate roles, and oversight and regulatory functions. For example, His Majesty's Inspector of Constabularies and Fire and Rescue Services (HMICFRS) are not an oversight body, as claimed by the Minister. Moreover, limitations of some of the above named police bodies to perform meaningful regulatory oversight were recently and comprehensively laid out in Baroness Casey's independent review into the standards of behaviour and internal culture of the Metropolitan Police Service,

[187] Interview with Chief Constable Charlie Hall, Hertfordshire Constabulary and National Police Chiefs' Council lead for ANPR
[188] Interview with Assistant Chief Constable Jenny Gilmer, South Wales Police, National Police Chiefs' Council lead for CCTV.
[189] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf p.273

> *"The structures of governance and scrutiny are relatively weak. HMICFRS are an inspectorate not a regulator and can only really comment on what they find. They have limited levers to drive improvement. The 'engage' phase is a reflection of the Inspectorate's significant concerns about the force, but it holds no real consequences for the Met."*[190]

In addition, without further specific legislation it can be argued that the Equality and Human Rights Commission (EHRC) are not currently constituted to legitimately address many of the functions and activities outlined above and the totality of surveillance oversight needs. Added to this, the 'regulatory' reach of the EHRC in this area can be judged by the fact that in March 2020 this organisation called to suspend the use of facial recognition in England and Wales "until their impact has been independently scrutinised and laws are improved",[191] with no impact on the continued use of this technology.

The previous Surveillance Camera Commissioner, expressed that,

> *"I don't believe the EHRC have the reach to legitimately get involved in this type of work. I think they need to be supported by legislation, not just general legislation, or not general human rights legislation which covers the world and every element within it."*[192]

This point was echoed by Professor Lorna Woods, an academic expert on digital law, "I don't think that the Equalities and Human Rights Commission actually has the formal detailed oversight role".[193] Reflecting the aforementioned issue of dedicated specialism, the previous Surveillance Camera Commissioner added,

> *"What we're looking at is surveillance and, as you know, surveillance is a specialist area. It's grown exponentially, and we've seen not just the overlap between biometric surveillance and but the more complex surveillance which is multi sensor surveillance. Now it's easy for non specialists to lose themselves getting into the morass of this kind of issue, and not do what my [former] role is intended to do, which was to drive standards north."*[194]

This sentiment was echoed by the current Scottish Biometrics Commissioner who regarded the EHRC remit as 'too broad'.[195] A representative from the Scottish Biometrics Commissioner's office elaborated on the exceptional status of policing in the context of other public bodies,

> *"I think what the UK Government is forgetting here is an important distinction, which is that policing purposes are very different from most of the other public bodies when it comes to what they do. The police by his own nature is very intrusive and they require special oversight bodies to cover them. We're talking about accountability mechanisms, governance frameworks, safeguards, all these things, [rather] than by then a body that focus only on compliance, data protection, or that only focuses on human rights in general. So, to be specific, at the moment in terms of expertise, and in terms of political influence, I don't think the EHRC are there institutionally at the moment."*[196]

---

[190] Baroness Casey Review (2023) Final Report: An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service, available from https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/baroness-casey-review/update-march-2023/baroness-casey-review-march-2023a.pdf p.15.

[191] Equality and Human Rights Commission (2020) Facial recognition technology and predictive policing algorithms out-pacing the law, available from https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law

[192] Interview with Anthony Porter, former Surveillance Camera Commissioner.

[193] Interview with Professor Lorna Woods.

[194] Interview with Anthony Porter, former Surveillance Camera Commissioner.

[195] Interview with Scottish Biometrics Commissioner.

[196] Interview with Diego Quiroz, Operations Manager, Scottish Biometrics Commissioner.

Oversight through the FIND-SB Board

Another suggestion has been that the FIND-SB board could fill the oversight role vacated by the BSCC.[197] As mentioned earlier, the Bill Explanatory Notes also make provision for extending the board's focus beyond DNA and fingerprints to encompass other biometric material such as facial images.

One difficulty with this position is that while the FINDS board overlaps with issues of biometric oversight it does not necessarily provide that oversight in itself. Indeed, the presence of the BSCC on the board is one of the ways in which it offers oversight. For example, core constituencies on FINDS board membership appear to be the Home Office, who fund and develop data infrastructure; the police, who collect and manage data; and regulators/oversight bodies. Removal of the BSCC would therefore weaken its oversight capability.

The Forensic Science Regulator, himself a former chair of the FINDS board (in its previous incarnation) explains,

> *"effective operation [of the FINDS board] relies on the work of FINDS Unit in the Home Office and the data and information they produce and present to the Board. This data and information has broadened and improved over the years and I think the work that has been done on error rates is exemplary. Having a strategic forum like this where a collective view can be taken of scientific standards, legality, ethics and privacy is not only critical in scrutinising the use of forensic databases but critical to their future development and ensuring that appropriate governance is built into new technologies, science and biometrics".*[198]

Key here is the emphasis on reaching 'a collective view' incorporating the stated range of perspectives. The Scottish Biometrics Commissioner, a FINDS board member, also raised how the removal of the BSCC from the FINDS board would reduce oversight. He also added that this would also remove an important expert voice from the body,

> *"If you don't have independent people sitting around the table to challenge that, then [there's the risk of portraying] everything's fine. Nothing to see here. The challenge at that forum at the moment, is from myself and [the BSCC]. But if you take away our major UK players, i.e. like the biometrics and surveillance camera Commissioner for England and Wales, at the same time, my voice becomes much weaker at that forum… The board can't replace a biometrics commissioner."*[199]

Two other points are relevant here. The first, related, issue is that of independence. Clause 106(11)[200] of the Bill suggests amendments to the Section 63AB of the Police and Criminal Evidence Act 1984, the section covering the National DNA Database Strategy Board. Among other changes is the following proposal:

> (11) At the end [Section 63AB of the Police and Criminal Evidence Act 1984] insert—
>
> (10) The Secretary of State may by regulations made by statutory instrument—
> (a) change the databases which the Board is required to oversee by—
> (i) adding a database operated for policing purposes which consists entirely or mainly of biometric data,
> (ii) removing a database;
> (b) rename the Board;
> (c) require or authorise the Board to issue a code of practice or guidance.

[197] See above and Bill Explanatory Notes available here: https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf
[198] Written submission from the Forensic Science Regulator.
[199] Interview with Scottish Biometrics Commissioner.
[200] Clause 113 in the version amended after Commons Public Bill Committee stage.

(11) Regulations under subsection (10) may —
(a) amend this section;
(b) make different provision for different purposes;
(c) make consequential, transitional, transitory or saving provision.

The wording of Clause 106 thus appears to offer the Secretary of State considerable latitude for altering the parameters and function of the FINDS board. Coupled with the removal of the BSCC role and membership of the board – and the consequent re-balancing of membership towards a higher proportion of police and government membership – this raises significant questions over the independence of the board if it is to offer meaningful impartial oversight.

The second issue concerns the agility of the FINDS board mechanism. According to the current BSCC, (currently unpublished) minutes from the latest FINDS Board held during Summer 2023 contained outstanding actions raised by Professor Paul Wiles, the previous Biometrics Commissioner.[201] This would mean actions such as this are over three years old, thus generating questions over the level of adaptive and responsive oversight brought by this mechanism.

[201] Stated in personal correspondence with the BSCC, August 2023.

CONCLUDING REMARKS

The Data Protection and Digital Information Bill proposes substantial changes to the oversight of overt surveillance and biometric materials in addition to the regulation of data processing. This report offers a detailed analysis of these changes and, drawing on insights from senior practitioners and other experts, concludes that, if enacted in current form, the Bill will create significant gaps in the oversight of existing uses of surveillance cameras and biometric materials. In addition, the capacity to address future challenges associated with increasingly sophisticated and digitally advanced surveillance tools will be depleted. Such outcomes have obvious impacts for the fundamental rights of individuals but are also likely to complicate the work of those legitimately using technologies to keep the public safe.

Moreover, the arguments used to justify such changes, including the claim that sufficient and comparable oversight exists elsewhere, are found to be wanting. They also and fail to recognise the complexities of the current regulatory landscape and the protections offered by the BSCC in an era of increasingly intensive advanced and intrusive surveillance.

This report sets out in detail the roles, activities and functions that will be lost, and the gaps in oversight that will arise, with the abolition of the BSCC role. The following advances some considerations over future directions for maintaining and enhancing oversight in this area.

It is essential that the SCCoP, or some variant thereof, along with a designated vehicle to ensure compliance, is retained. The Code and its attendant compliance-related activities are heavily embedded into the work of local authority surveillance camera operators and managers, police and other public bodies. Widespread support for these measures exists across this range of practitioner communities and the Code is unequivocally seen as a means to raise standards. Of further note is the diffusion of benefit brought by the Code. The institution of the Code, and the requirement for surveillance practitioners to regard it, has initiated a wide range of valued activities that support better practice across the sector.

This report does not advocate that current arrangements are sufficient for addressing the range of challenges that lie ahead. However, the proposals forwarded by the DPDI Bill represent a removal of many key oversight activities and processes that do exist. Any belief that the range of activities aimed at raising standards outlined above would be taken up or equivalenced by other organisations, and without a clear designation of responsibilities and resources, is unrealistic.

The current moment is a time of accelerated innovation in the scale and capability of surveillance technology. This is particularly heralded by advancements in biometric surveillance. Concerns have simultaneously arisen over surveillance technologies (and AI in general) to the extent that they have now become mainstream issues. These issues are not going to go away. Additional to this, are heightened challenges for policing agencies and other public bodies to regain public trust and confidence. Considering these issues together raises questions over the added impact of removing oversight at this specific time. Debates around surveillance are often, and unnecessarily, polarised and divisive. Rolling back oversight at this time is highly likely to split the debate further, making it more challenging for surveillance users to gain trust, legitimacy and support within the communities they aspire to serve.

Echoing calls from leading experts and an opinion issued by the then Information Commissioner Elizabeth Denham, the regulatory basis of oversight policies and codes should be strengthened so they become legally binding and include provision for meaningful enforcement. This would avoid any prospect or perception of 'cherry picking' convenient parts of the growing library of guidance and well-meaning yet legally unenforceable digital ethics principles (or similar). Another

benefit would be that such a Code could be adapted to accommodate emerging technologies. A stronger, legally enforceable, regulatory basis would bring clarity and certainty to how rapidly developing technologies could be used in accordance with the law.

Added to this, the retention of an annual public reporting mechanism is essential to the maintenance of transparency and accountability. Such activities add meaning to often stated aspirations for 'surveillance by consent' and the promotion of public trust, and hence legitimacy, for public surveillance activities.

Taking the above into account suggests some value clearly exists in exploring the retention of the BSCC role in some capacity and, in the authors' view, strengthening it to accommodate future oversight challenges. This would also capitalise on the positive and effective engagement that already exists between the BSCC and surveillance developers and users. This position is further supported by the limitations in many of the arguments advanced to abolish the role, which are analysed in detail in this report.

If the SCCoP were to be retained in some form, abolishing the BSCC role begs the question of where it should be located, and where responsibility to its enforcement lies. Of consideration here are the range of functions attached to the existing code, the possibilities for adaption, requirement for annual reporting and the necessity of technological expertise among regulators. Moreover, surveillance is not reducible to data protection, particularly in an era of advanced-AI enabled tools.

Should the role and associated functions be abolished, a next obvious venue for oversight to explore is how the Investigatory Powers Commissioner's Office (IPCO) may be well placed to adopt some of these functions. This is particularly relevant if the SCCoP is to be retained (which this report argues is crucial to maintaining basic standards of oversight in this area). Established in 2018, IPCO has well-instituted practices focused on the authorisation of intrusive surveillance techniques, in addition to carrying out inspection and review roles, three activities that cover the lifecycle of surveillance operations. IPCO is continually faced with innovative surveillance technologies and techniques and, in addressing them produces regularly updated guidance for staff and has a standing expert technology advisory council. Under the DPDI Bill IPCO look set to inherit some limited biometric casework functions. Bringing the wider range of activities into an expanded IPCO would not only desegregate the oversight of biometric surveillance it would also anticipate and better address future challenges over increasingly blurred lines between overt and covert surveillance. Moreover, under the stewardship of its first permanent Commissioner, IPCO devised a public reporting mechanism that revealed unprecedented detail on the activities of intelligence agencies, while maintaining operational integrity. Given the heat and polarisation of public debates around surveillance and its impacts, appealing to such a range of professional and public communities looks more important than ever before.

ANNEX I: INDIVIDUALS INTERVIEWED AND CONSULTED WITH FOR THE INDEPENDENT REPORT

John Bonney, CCTV Lead, Intervention and Prevention, Blackburn and Darwen Borough Council, Incoming Chair of the Public CCTV Managers Association

Alex Carmichael, Chief Executive, Security Systems and Alarms Inspection Board (SSAIB), National Strategy for Surveillance Cameras Strand Lead for Standards and Certification

Deputy Chief Constable Jim Colwell, Devon and Cornwall Police. National Police Chiefs' Council lead for Body-Worn Video

Assistant Chief Constable Jenny Gilmer, South Wales Police, National Police Chiefs' Council lead for CCTV

Tony Gleason, CCTV Manager, Bournemouth, Christchurch and Poole Council. Outgoing Chairperson of Public CCTV Managers Association

Chief Constable Charlie Hall, Hertfordshire Constabulary and National Police Chiefs' Council lead for ANPR

Alison Lowe OBE, Deputy Mayor for Policing and Crime for West Yorkshire

Professor Carole McCartney, Professor of Law and Criminal Justice, University of Leicester

Mark Norris, Principal Policy Adviser, Local Government Association

Professor Marion Oswald MBE, University of Northumbria. Member of the Independent Advisory Board of the Centre for Data Ethics and Innovation.

Brian Plastow, Scottish Biometrics Commissioner

Anthony Porter OBE, former Surveillance Camera Commissioner

Gary Pugh OBE, Forensic Science Regulator. Former Director of MPS Forensic Services

Dr Joe Purshouse, Senior Lecturer in Law, Sheffield University

Diego Queiroz, Office of the Scottish Biometrics Commissioner

Tim Raynor, Video Surveillance Product Manager UK&I. Vice chair for the Video Surveillance Section, British Security Industry Association (BSIA)

Andy Read, South Wales Police, National Police Chiefs' Council National Capabilities Manager for CCTV

Professor Fraser Sampson, Biometrics and Surveillance Camera Commissioner

Gordon Tyerman, Managing Director, CCTV Training and Logistics. National Strategy for Surveillance Cameras Strand Lead for training

John Wadham, Human Rights Advisor to the Northern Ireland Policing Board

Professor Lorna Woods OBE, Professor of Internet Law, University of Essex

Additional interviews were conducted with individuals who requested anonymity and are therefore not quoted or listed here. These included senior experts on matters of data protection and policing. Additional to the above, are the many additional experts and practitioners that provided background information and those who reviewed the report prior to submission. The authors are extremely grateful for the generosity of all contributors in offering their time and insights for this report.

ANNEX II: NON-EXHAUSTIVE LIST OF REGULATORY AND OVERSIGHT BODIES RELEVANT TO SURVEILLANCE AND BIOMETRICS

Acronym	Name	Legislation Establishing the Role	Notes	Jurisdiction
ICO	Information Commissioners Office	Data Protection Act 1984	Legislation replaced by the Data Protection Act 1998 and Data Protection Act 2018. The latter codifies elements of the EU GDPR into UK Law. The ICO remit covers both public and private entities	UK wide
SCC	Surveillance Camera Commissioner	Protection of Freedoms Act 2012		England and Wales
BC	Biometrics Commissioner	Protection of Freedoms Act 2012		Split. Some judicial functions (e.g. National Security Determinations on the retention of biometric data) are UK-wide. Others, such as those covering police uses of biometrics are limited to England and Wales
BSCC	Biometrics and Surveillance Camera Commissioner	Protection of Freedoms Act 2012	The SCC and BC roles were undertaken by the same individual in 2021	As above for the SCC and BC roles
SBC	Scottish Biometrics Commissioner	Scottish Biometrics Commissioner Act 2020		Scotland
IPCO	Investigatory Powers Commissioner's Office	Investigatory Powers Act 2016		UK-wide
EHRC	Equality and Human Rights Commission	Equality Act 2006		Great Britain (England, Scotland and Wales)
FINDS Board	Home Office Forensic Information Databases Board (formerly the National DNA Database Strategy Board).			
HMICFRS	His Majesty's Inspector of Constabularies and Fire & Rescue Services	County and Borough Police Act 1856, key statutory duties defined in the Police Act 1996		
FSR	Forensic Science Regulator	Established in 2007. The role was not established by statute. The FSR was made statutory by the Forensic Science Regulator Act 2021.	The Forensic Science Regulator Act 2021 included a requirement for the FSR to produce a code of practice (approved by Parliament March 2023, comes into force October 2023).	

ANNEX III: INTERIM REPORT SUBMITTED AS EVIDENCE TO THE HOUSE OF COMMONS PUBLIC COMMITTEE STAGE OF THE DATA PROTECTION AND DIGITAL INFORMATION BILL (11 MAY 2023)[202]

1. Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. These new and advancing technologies hold clear potential to enhance public safety yet also have the capacity for enormous harms. The possibilities for integrated surveillance technology, driven by AI and supported by the internet, create genuine public anxieties over civic freedoms. These anxieties exist across almost all jurisdictions. Within this context, consideration of genuine, meaningful and trustworthy governance and oversight is urgent and pressing.
2. In current form, the Bill will delete several surveillance oversight activities and mechanisms that are set out in legislation and arise from the fulfilment of statutory duties placed on Commissioners. Prominent among these is the tabled abolition of Protection of Freedoms Act 2012 (POFA) legislative requirements to (a) appoint a Surveillance Camera Commissioner and (b) to publish a Surveillance Camera Code of Practice, which offers governance coverage far beyond data-related issues. The Code is realised through the national Surveillance Camera Strategy, which would also disappear. The value of the Code and Strategy for providing surveillance oversight, raising standards in surveillance practice, delivering guidance for camera users, and offering transparency and public confidence is set out in more detail below.
3. The other functions of the Biometrics & Surveillance Camera Commissioner are manifold and comprise both judicial and non-judicial elements. Key activities and benefits include, but are not limited to developing, and encouraging compliance with the Code; raising standards for surveillance camera developers, suppliers and users; public engagement, and building legitimacy and consent for surveillance practices; annual reporting to Parliament via the Home Secretary; convening expertise to support these functions; reviewing all National Security Determinations and other powers by which the police can retain biometric data.
4. Surveillance oversight is historically and currently overburdened and under-resourced. Activities undertaken by the SCC component have extended the Commissioner's role, not in terms of regulatory overreach, but to compensate for this shortfall, thereby raising standards and increasing professionalism across the sector. While not defined in the original legislation (POFA), these activities have arisen *as a result of successive Commissioners fulfilling their statutory duties*. The Bill proposes the erasure of many such functions and, by extension, their associated value to society. As one expert interviewee for the report expressed, having been based on a consultation about 'absorption' of the functions by the Information Commissioner "the Bill makes no provision for absorption whatsoever. It just deals with extinction". For example, the Bill contains no provision for continuing the work of driving up standards for the development, procurement, adoption and use of surveillance cameras, a programme of work widely applauded across police, practitioner and industry communities.
5. The value of these activities is widely recognised and easily evidenced across civil society organisations, industry professionals, Parliament, and law enforcement communities. Of the latter, it is important to acknowledge significant evidence of (a) police support for the SCC role and (b) requests for clarity over appropriate uses of surveillance tools.
6. The POFA Commissioners' functions are not regulatory in the same sense as the Information Commissioner (ICO). This difference has several implications. First, the roles are not directly comparable with ICO. Consequently, the impact of SCC functions arises through different and sometimes less visible or direct means. It also means elements cannot be directly "lifted and

shifted" into a different regulatory format and destination.

7. Also crucial is that these activities extend significantly beyond matters of data use. Considering surveillance impacts and harms purely in terms of data protection is widely recognised as a highly restrictive and selective framing. It is also widely acknowledged that rights concerns arising from surveillance are not reducible to issues of privacy alone. One could further argue that adding POFA to the existing data protection landscape constituted recognition of this over a decade ago.
8. Advanced digital surveillance, particularly AI-driven forms, is a global phenomenon. The Bill's reduction of surveillance-related considerations to data protection compares unfavourably to regulatory approaches in other jurisdictions. Many have started from data protection and extended to cover other germane issues. Examples include EU proposals around an AI Commissioner, and the MEP vote to support a compromise text for the AI Act that bans public uses of remote biometric identification (including facial recognition) on 11 May 2023.
9. Examples of these wider activities and their impact are:

a. The BSCC's recent success in addressing widespread use of Chinese cameras with known cyber vulnerabilities in sensitive UK sites. The development of these tools is also associated with significant human rights abuses.
b. Automatic Number Plate Recognition (ANPR) surveillance operates on one of the largest databases in Europe. It has grown from a local to a national network, from focused counterterrorism uses to monitoring urban clean air zones and car park ticketing. Credible estimates suggest a likely 100 million daily ANPR data acquisition points from 2024. ANPR grew with little data protection-related scrutiny. The SCC role brought proactive engagement that established an independent advisory group to provide standards and governance for this technology, and to convene key stakeholders (including the police) into this activity.
c. SCC established current guidance to law enforcement concerning lawful and ethical use of facial recognition. This guidance transcended data protection issues, addressed standards, transparency, ethics, human decision-making and the authorisation of deployments. It is now incorporated into NPCC guidance.

10. The Bill removes reporting obligations currently in POFA Commissioner roles. This removes a mechanism for assuring Parliament and the public of appropriate surveillance use, affecting public trust, and legitimacy invested in surveillance practices. We are at a critical moment concerning public trust in institutions, particularly law enforcement, something central to the success of UK policing. As drafted, the Bill reduces public visibility and accountability of related police activities.
11. The independence of oversight is similarly crucial to public trust. Clause 28 of the Bill requires the new Commissioner to respond more explicitly to "strategic priorities" designated by the Secretary of State. This may risk diluting public trust and confidence in the paramount condition of independent oversight.
12. The Bill seeks to transfer some responsibilities outlined in POFA (fingerprints and DNA) to other entities, allow others to lapse, and makes no provision to the functions and oversight activities arising from several POFA Commissioner duties. One argument has been that many SCC activities are not defined in POFA and therefore cannot be transferred. However, the Code enables the SCC to provide and issue guidance across the surveillance landscape. It also requires 'relevant authorities' to comply with its principles. These are two powerful requirements which hold state institutions to account yet the Code is to be deleted. Several issues arise from this decision to restrict formal transfer of only those biometric responsibilities specified in POFA and deleting anything relating to surveillance camera standards:
13. Biometric technology is expanding and diversifying at an unprecedented rate. Specifying only

those biometric techniques mentioned in legislation of over a decade ago challenges notions that the Bill is "future proofed". By designating fingerprints and DNA to the Investigatory Powers Commissioner (IPCO) also risks a de facto segregation in the oversight of different biometrics techniques, where the governance of all other forms rests elsewhere. It removes any statutory duties from the interface of biometrics and surveillance, the policy basis on which ministers recently combined the POFA Commissioner functions. Moreover, one could argue that given the potential for collateral intrusion, remote biometric surveillance resonates more closely with IPCO's remit than fingerprints and DNA.

14. The original proposal consulted on was for all POFA biometric and overt surveillance functions to be absorbed by the ICO. The Bill reflects the view of many that biometric casework sits more naturally with IPCO. Expert interviewees for the report highlighted how most gaps left by this Bill could also be addressed if responsibility for the Surveillance Camera Code (only recently approved by Parliament) also moved under IPCO. This would harmonise all functions for oversight of traditional and remote biometrics in policing under one established and internationally regarded judicial oversight body. Such a move could also add genuine 'future proofing' by anticipating the increasing potential for blurring boundaries between overt and covert surveillance brought by new advances in technology.
15. Academic research has demonstrated significant public concern over one such form of remote biometric monitoring, facial recognition technology. Other experts and public bodies have called for more detailed rules for uses of this technology in public. A stark contrast exists in the working of the Bill between mention of relatively uncontroversial decades old biometric techniques and the cutting-edge technologies currently animating public debate. Reference to "remote biometric identification" could be one entry point to addressing this issue.
16. This issue is made more pressing given the Policing Minister expressed his desire to embed facial recognition technology in policing and is considering what more the government can do to support the police on this. Such embedding is extremely likely to include exploring integration of this technology with police body worn video (interview with the BSCC)
17. Excluding IPCO, expert interviewees questioned the suitability of alternative venues for surveillance and biometric oversight. This issue invokes several considerations. One concerns thematic coverage and the spectrum of potential surveillance harms that transcend data-related matters. Additionally, two organisations have been highlighted as possible venues for absorbing public surveillance oversight functions: a modified Information Commissioner's Office and, separately the Equality and Human Rights Commission. Taking these in turn, POFA oversight is mostly limited to the activities of public bodies. Existing data protection regulation covers both public and private entities. Housing oversight in the later may provide wider scope and address complexities of regulating public-private surveillance activities. However, research has demonstrated the limited role data protection controllers have played in providing enforcement against breaches in relation to video surveillance in a significant number of countries including the UK. In addition, without further specific legislation the EHRC are arguably not currently constituted to legitimately address many of the functions and activities outlined above and the totality of surveillance oversight needs.
18. It is widely accepted that current oversight of complex surveillance practices is considered patchy and requires simplification. Simplifying oversight has been consistently stated as a key aim for the Bill. However, such simplification entails at least three further considerations:

a. Calls for simplified oversight correctly include a requirement for companion policies for implementation and compliance. These translate abstract principles into clear guidance and standards for users of biometric and other surveillance technologies while offering mechanisms for auditing compliance. This relationship between law and policies was central to

the *Bridges* Court of Appeal judgement on facial recognition technology in light of which the Home Secretary amended the Code. The Bill contains no mention of guidance or compliance mechanisms aside from those pertaining to data management. The absence of requirements for guidance and to ensure compliance generates vulnerabilities for users of these technologies and for the rights of individuals subjected to them, and is particularly important given the significant uncertainties brought by emerging technologies.

b. Simplification is an important ambition but should not come at the expense of meaningful oversight. For example, as one expert interviewee remarked, "why is it that simplification is more important than raising standards?"
c. What may appear a simplification in organisational terms does not naturally translate into a simplification in a practical sense. As stated above regarding different biometric techniques, this ambition for simplification may actually complicate the oversight landscape. Removing a Commissioner who proactively interfaces with developers and users of surveillance technologies may generate future difficulties. For example, it may take longer for aspiring technology users to access knowledge. In addition to impacting public resources, pressing ahead with surveillance deployments before such advice is received may generate greater exposure to litigation for public bodies. Alternatively, the absence of such information may lead users to highly conservative interpretations of the law which may dissuade legitimate uses of surveillance technology for public safety.

Professor Pete Fussey and Professor William Webster, 11 May 2023