DCMS Consultation: "Data: A new direction"
Response by the Biometrics and Surveillance Camera Commissioner

1. Introduction

1.1 The Commissioner for the Retention and use of Biometric Material and the Surveillance Camera Commissioner are independent appointments each made by the Home Secretary under the respective provisions of the Protection of Freedoms Act 2012 (the Act)[1].

1.2 In March 2021, the Home Secretary appointed me to both roles as expressly recognised in para 4.10 of the consultation. This dual appointment meant that, while remaining legally discrete, the statutory functions of the two roles are now the responsibility of a single individual. To that extent I personify a 'simplification' of the framework governing the police use of biometrics and overt surveillance although, in discharging the relevant functions, I must nevertheless take account of the statutory parameters and distinct responsibilities of each.

1.3 The issues around the appropriate regulation and oversight of the police use of biometrics and surveillance have been under consideration for several years and the case for reform has featured in the statutory annual reports of both commissioners; they have also arisen in parliamentary scrutiny and in correspondence held by my office. It is clear to me from that correspondence that a motion to appoint a single individual in the Information Commissioner's Office (ICO) to be responsible for these existing statutory functions was originally explored in 2020 and that a perceived lack of transparency around the process created significant concern for both of my predecessors.[2] The arrangements to put the appointment into effect appear to have reached an advanced stage when they came to the attention of my predecessors, at which point the former Biometrics Commissioner wrote directly to the Information Commissioner about it.[3] While I can find no record of any definitive decisions having been taken the exchanges serve to underscore the need for transparent decision making, something that is particularly acute if public trust is to be maintained in the independent regulation and oversight of police use of biometrics and surveillance. For all the reasons set out in the most recent report of the Committee on Standards in Public Life[4] any remaining matters preceding my appointment should be reviewed and the lessons identified.

2. The Question of Consultation

2.1 The present consultation by the Department for Culture, Media and Sport (DCMS) is the second of two back-to-back consultations by the government that affect my statutory roles and functions. The first was the statutory consultation[5] on the Home Secretary's revised Code of Practice for surveillance camera systems in August of this year. Led by the Home Office, this consultation proposed several changes to update

[1] Ss 20(1) and 34(1) of the Act
[2] See, for example, letter from Surveillance Camera Commissioner Tony Porter 16 April 2020
[3] Letter from Biometrics Commissioner, Professor Paul Wiles 11 May 2020
[4] www.gov.uk/government/publications/upholding-standards-in-public-life-published-report
[5] Required under s.31(2) of the Act

the Code and I was directly involved in its drafting and publication as a statutory consultee[6]. That consultation concluded on 8 September 2021 and I published my formal response[7] without any knowledge that there was to be a further consultation some two days later on the transfer of my statutory functions to the ICO.

2.2 On 10 September 2021, the government announced this consultation on data reform. Until it was brought to my attention privately, I had been wholly unaware of the consultation or the fact that it was to contain a question about the transfer of functions to the ICO. At the time of writing I have yet to receive formal notification as a statutory officeholder but, notwithstanding that formality, I have had the advantage of seeing the letter sent to other stakeholders and have met with officials and the Minister for the Lords for which opportunities I am grateful[8].

2.3 Coming at the very end of what is a detailed document, the consultation questions (5.8.1 & 2) seek views on the government's exploration of "the potential for further simplifying the oversight framework by absorbing the functions of [the Biometrics and Surveillance Camera Commissioners'] roles into the ICO". Given that the process to transfer the existing functions to an individual working within the ICO had already begun before my appointment one might be forgiven for thinking that the government has already answered its own questions and the consultation gives the appearance of putting the deliberative cart before the determinative horse. As the independent officeholder for both statutory roles I am bound to ask whether those actions and the recorded concerns of my predecessors ought to have been made clear in the consultation itself, particularly as the consultation document contains other substantial sections where the government's intention is unequivocally expressed[9] or where more than one option is put forward[10]. Having now seen the extent of the proposed revisions to the Surveillance Camera Code of Practice and the questions in this current consultation I can understand why some stakeholders may believe this to have been a mere formality.

2.4 I have raised these issues with officials and also with my team and I appreciate the difficult position in which they can find themselves when trying to provide accurate information while at the same time not wishing to encroach on my independence. Crucially I have received a categorical assurance from ministers that the purpose of the consultation questions is to enable the proper formulation of as yet undecided policy in light of informed responses. It is on that understanding that I submit this one.

3. The Consultation Question

3.1 I rarely come across people arguing that we need more regulators. Businesses and public services alike recognise the real burdens of an overregulated landscape as

[6] Under s.29(5) of the Act. The ICO is also a statutory consultee under this provision

[7] www.gov.uk/government/organisations/surveillance-camera-commissioner

[8] I note without irony that both consultations are aiming for simplified and joined-up governance in this field but neither consultation makes reference to the other, nor to the 2020 decision to transfer the functions to an individual within the ICO.

[9] See, for example, paras 237 and 238

[10] See, for example, paras 91 and 121

reflected in the government's One In-One Out rule for regulators first published in 2011[11]. That same approach seems to be the crux of the proposed data reform programme set out in the consultation generally. What most people with whom I come into contact in my current dual role ask for is *better* regulation. That may mean *simpler* and *stronger* regulatory frameworks with powers of enforcement, it may even mean the introduction of regulation for areas currently left to self-determination. It is worth noting that, after hearing from the Biometrics Commissioner and the Information Commissioner, in 2015 the House of Commons Select Committee on Science and Technology recommended that governance would be improved by *extending* the statutory responsibilities of the Biometrics Commissioner "to cover, *at a minimum*, the police use and retention of facial images. The implications of widening the Commissioner's role beyond facial images should also be fully explored, costed and the findings published"[12].

3.2 In my experience the *best* regulation usually involves intuitive arrangements where responsibility is to be found where you would think of looking for it and where, once found, the avenues for engaging are easy to navigate and encourage meaningful contribution. Better regulation is an ambition of the consultation as a whole and is no less important in the final two questions than elsewhere. However, those consultation questions (the 'Home Office' questions) ask for views only on two very narrow things that directly affect the functions of my office:

3.2.1 simplification of the oversight framework for *police* use of biometrics and *overt* surveillance (Q 5.8.1) and

3.2.2 'absorption' of the statutory functions under a 'single oversight function' by the ICO (Q5.8.2).

3.3 Before submitting a response to them I would make several observations about the questions themselves.

3.4 It should be noted that the current oversight framework for overt surveillance also covers the operation of CCTV and other surveillance camera systems by *local authorities*[13] as they are 'relevant authorities' under the Act and as such have a legal duty to have regard to the Surveillance Camera Code of Practice. This point has been overlooked in the questions. The reference to the police use of *overt* surveillance deliberately excludes the existing role and functions of the Investigatory Powers Commissioner which is not only an arguably more valid alternative to the proposed option of the ICO (see below), but also one that has been proposed by previous Biometrics and Surveillance Camera Commissioners.

[11] assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/48179/2836-onein-oneout-statement-new-reg.pdf; accessed 5 October 2021

[12] publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf; Current and Future Uses of Biometric Data and Technologies 6th Report of Session, 25 February 2015 at para 105; accessed 8 October 2021

[13] S.33(5) of the Act

3.5 The second question simply asks for views about the 'absorption' of the functions under the ICO rather than offering alternatives (as found elsewhere in the consultation); it also speaks of "data for biometrics" which is an odd expression and one that appears to place emphasis on the 'data' element rather than the biometric "material" which is the statutory language in this area.

3.6 The Oxford English Dictionary reminds us that "absorb" can mean "*to understand fully*" as well as simply 'take over' and before considering the implications of absorption of any statutory functions, it is necessary first to understand fully what those functions are and their relevance to policing, law enforcement and national security.

4. Independence

4.1 The need for independent commissioners was considered and enacted by Parliament in 2012. The principal intention of that part of the Act was to provide an *additional* layer of independent scrutiny, oversight, guidance and, in the case of biometric material, intervention over and above that supplied by the general framework for upholding basic information rights of the individual.

4.2 When the Protection of Freedoms Act 2012 was being passed in the UK, one US researcher described how we were witnessing an emerging series of "next generation biometrics, such as hand geometry, iris, vascular patterns, hormones, and gait, which, when paired with surveillance of public space, give rise to unique and novel questions of law and policy".[14] She goes on to describe how these next generation capabilities - which have been raised consistently with ministers and Parliament by my predecessor[15] - "constitute what can be considered Remote Biometric Identification (RBI). That is, they give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner. As such, RBI technologies present capabilities significantly different from that which the government has held at any point in [U.S]. history."

4.3 Since then the technology, its use and most importantly the public demand for greater safeguards have changed beyond most informed prediction. At that time Edward Snowden had yet to become a household name in state surveillance matters[16] and was still working as a contractor for the NSA. As set out in the press release announcing its independent review of the governance of biometric data last year, the Ada Lovelace Institute noted that "technologies which capture, analyse and compare biometric data are increasingly being used by police, public authorities but a lack of regulation of these technologies has led to public protest, legal challenge and calls for action from the House of Commons Science and Technology Committee[17]. At the time

[14] Laura K. Donohue, "Technological Leap, Statutory Gap, and the Constitutional Abyss: Remote Biometric Identification Comes of Age" (2012) 97 *Minnesota Law Review* 407, 415.

[15] Biometrics Commissioner calls for debate in wake of Home Office strategy report – Risk Xtra (risk-uk.com) accessed 5 October 2021

[16] www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[17] Adalovelaceinstitute.org, 24 January 2020

of writing, the results of the review, conducted by Matthew Ryder QC, are expected imminently.

5. Biometrics and Surveillance Functions

5.1 As Biometrics Commissioner I have two *quasi-judicial* functions, the first being the review of all National Security Determinations (NSDs).

5.2 Made by chief police officers, NSDs are highly exceptional measures that are used to retain the biometric material of individuals who, while never having been convicted of *any* offences, are nonetheless believed to present such a threat to our national security that retention of their biometrics is deemed necessary by the police and the Security Service. The making of an NSD represents a substantial and enduring interference with the rights of the subject particularly as they are not informed of its existence and have no opportunity to make representations to me or anyone else. The criteria for making and reviewing NSDs are necessarily very strict and every NSD must be reviewed by me as Biometrics Commissioner. If I am not satisfied that the NSD has been properly made I have the statutory power to order destruction of the biometric material. The NSD process is managed through the national secure network for counter-terrorism policing and involves detailed consideration of intelligence of the utmost sensitivity. Chief officers making NSDs have a legal obligation to have regard to any statutory guidance published by the Home Secretary[18] and I am a statutory consultee, along with the Lord Advocate[19].

5.3 Recent developments have underscored the importance of having effective dynamic mechanisms for countering international terrorism and the use of NSDs – particularly as part of the arrangements under Schedule 7 to the Terrorism Act 2000 - is critical to the effective working of those mechanisms[20]. Again, the Biometrics Commissioner must report annually to Parliament on the use and operation of this extraordinary statutory power by the police working in close consultation with the Security Service across England and Wales, Scotland and Northern Ireland. During 2018 and 2019 the Biometrics Commissioner reviewed more than 800 NSDs; he challenged for more information in 10% of those and in 2% ordered the destruction of the material held. Since I took up the role of Biometrics Commissioner in March 2021, I have already reviewed over 600 NSDs, have challenged many and have at the time of writing ordered destruction in 2 cases.

5.4 My second quasi-judicial function is to determine police applications to retain the biometric material of people who have been arrested for serious offences such as assault and sexual offences but where they could not be charged. This power is available to the police where the victim is particularly vulnerable such as in domestic abuse cases or offences against children and young people, as well as in other cases where the police believe that it is necessary to retain their biometrics to prevent or investigate crime. The type of scenarios where this has been used include cases where the victim is frightened to give evidence against a former partner or where the offence

[18] S.22(2) of the Act
[19] S.22(3) of the Act
[20] See Annual Report of the Biometrics Commissioner 2020/21

involves gang violence and the victim fears reprisals. In other words, it is used in some of the most challenging and high priority cases for policing at this time. These applications are also exceptional but are made regularly throughout the year for street robberies, burglaries, assaults and rape. The subject of the application is notified of it by the police and has a legal right to make representations to me. The chief officer then makes a detailed written application for consent to retain the biometrics. Without that consent the material cannot be retained. In Scotland this process is carried out by a judge. Unlike a judge, as an independent appointee, the Biometrics Commissioner produces an annual report to Parliament commenting on the use and outcomes of this statutory police power which applies to all police forces in England and Wales.

5.5 I also have the broader task of keeping under review the retention and use of DNA samples, profiles and fingerprints by the police, including the arrangements for exchanging biometric material with other countries, reporting annually on this to Parliament. The government's response to the pandemic raised concerns around a risk of temporary provisions 'bypassing Parliamentary scrutiny' and then becoming permanent[21]. One of my earliest responsibilities after being appointed was to review the impact of temporary legislation relaxing the governance restrictions on DNA and biometrics and to submit a report to Parliament accordingly[22], a report in which I was able to provide assurance as to the practices of the police and the risk of losing biometric material of individuals in a national security setting. A more enduring activity in discharging this role of assurance is visiting police forces to assess the extent to which the arrangements for the retention and use of biometrics by the police as set out by Parliament are being adhered to. In this aspect of my functions I work in an advisory and collaborative capacity.

5.6 None of these functions is 'regulatory' and in none of these settings am I there as a 'regulator'. This is an important point when considering the question of 'absorption' by a statutory regulator.

5.7 In my Surveillance Camera Commissioner role, I carry out a wide range of activities, which include:

5.7.1 chairing the Independent Advisory Group on Automated Number Plate Recognition (ANPR) a phenomenally powerful policing tool that registers some 60 million 'hits' per day and is used to support effective policing at neighbourhood, regional, UK and international level;

5.7.2 responsibility for the National Surveillance Camera Strategy working with leading experts in the fields of surveillance technology, practice and research; human rights law, critical national infrastructure considerations, ethics and public engagement;

5.7.3 working with the surveillance camera industry to explore the accountable, responsible and ethical use of new technology such as facial recognition and

[21] https://www.newstatesman.com/science-tech/2021/04/big-brother-watch-s-silkie-carlo-rule-law-has-broken-down; accessed 8 October 2021

[22] www.gov.uk/government/publications/regulations-made-under-section-24-of-the-coronavirus-act-2020

to enable the police and other law enforcement partners to harness new tools and techniques and visiting police forces to meet with their officers, staff and elected local policing bodies to understand how to collectively enable the responsible, proportionate and accountable exploitation of emerging tactical options in line with expectations of local communities and;

5.7.4 supporting the private sector in their voluntary adoption of the standards set out in the Code of Practice, from high street retailers like Marks & Spencer to operators of small drone businesses.

6. Biometrics, Surveillance and Data Protection

6.1 The lawful processing of personal data features in my functions as it does in every enterprise, public or private. In fact, it is difficult to identify a single public body that is able to carry out its functions without processing personal data, some of it very sensitive. To that extent basic processing of personal data has become almost a commodity, the proper processing of which is a necessary requirement of any organisational activity. As such its regulation requires consistent and coherent standards and application in much the same way as our health and safety regime, with clear guidance, policy and practice underpinned by, levers for ensuring compliance including enforcement and even prosecution.

6.2 A substantial amount of the data used by any surveillance camera system qualifies as 'personal data' and its lawful processing is principally a matter for the ICO. Biometrics and surveillance are usually deployed to identify (directly or indirectly) a living person by reference to an identifying feature, location data, or to one or more factors specific to their physical identity, physiological, mental, economic, cultural or social identity[23]. Therefore the concept of personal information is central to the legal framework governing biometrics and surveillance whether by the police or other bodies and the definition can include CCTV footage[24], personal images[25], fingerprints and DNA samples[26], a person's home address[27] and IP address[28] and vehicle registration plates[29]. Under the current arrangements, the lawful use by police of new surveillance technology such as live facial recognition[30] or of the Automated Number Plate Recognition (ANPR) system in England[31] or devolved areas of the UK[32] will generally involve broader data protection rights and remedies in the same way as data processing by other public services such as health, education and social care. In common with other public bodies the police are therefore already bound by generic

[23] All features of the definition in the General Data Protection Regulation European Union no. 2016/679.
[24] *Peck v UK* 44647/98
[25] *von Hannover v Germany (no 2)* 40660/08
[26] The storing of which amounts to an interference with subject's private life under the European Convention on Human Rights, Article 8 (*S. and Marper v UK loc cit*.
[27] *Alkaya v Turkey* 42811/06.
[28] *Benedik v Slovenia* 62357/14
[29] https://www.scotsman.com/news/transport/police-delete-half-billion-records-drivers-plates-1445560 accessed 26 August 2021
[30] See the grounds of challenge and appeal in *R (on the application of Bridges) v Chief Constable of South Wales Police and Ors* [2020] EWCA Civ 1058, many of which were determined on the application of generic data protection or public equality duty matters.
[31] https://www.independent.co.uk/news/uk/crime/royston-ring-steel-data-watchdog-warns-police-surveillance-scheme-rural-hertfordshire-town-unlawful-8730811.html
[32] https://www.scotsman.com/news/transport/police *ibid*

data protection laws and are subject to the ICO's very broad regulatory framework in the same way as any other data controller or processor including banks, estate agents or GPs.

6.3 But, 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.

6.4 As noted by both the United Nations and Interpol[33], 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. These policing purposes of the State are very different from the purposes of most other public bodies as expressly recognised within the domestic and international legal framework for data protection[34] and reflect the fact that 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. Some policing purposes increasingly involve the use of data gathered and processed by commercial organisations[35] or by citizens themselves, while aspects of the operational need to share biometric material - such as the international exchange of material between countries - are so complex and contentious that they require *combined* responsibility across my functions, those of the ICO and also the Forensic Science Regulator[36].

6.5 The nature of personal data processing needed in the effective prevention and investigation of serious crime, the prosecution of offenders and the protection of society from terrorism and other threats to national security is arguably of a different order to that used in the ordinary functions of most other organisations and public services. The police use of biometric data in the making of National Security Determinations, counter-terrorism policing and prevention 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 <u>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.</u>

6.6 Put shortly, there is an elemental difference between general data management principles and intrusive state surveillance; there are also fundamental considerations in this area that are not data protection issues at all.

7. Non-Data Protection Issues

[33] UNICRI and Interpol, Artificial Intelligence and Robotics for Law Enforcement, 2019, p. 2.
[34] Directive EU2016/680 the 'Law Enforcement Directive' which is given domestic effect in Part 3 of the Data Protection Act 2018
[35] http://privacyinternational.org/campaigns/unmasking-policing-inc; accessed 3 October 2021
[36] see Annual Reports of the Biometrics Commissioner: www.gov.uk

7.1 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.[37] 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. These potential consequences of routine surveillance are often referred to as 'chilling effects.' ... the risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance*[38]."

7.2 The impact on the fundamental human rights of the citizen and the so-called "chilling effect"[39] are central to the lawful (and acceptable – see below) operation of surveillance cameras[40] while, at the time of writing there is heightened public concern in the UK at the accountability of the police for unacceptable interference with the individual's right to protest and the potential effect of intrusive surveillance tactics[41] in particular on the citizen's right to express freely – or even to *hold* - political views[42]. The ability of mass surveillance to interfere with the most elemental of democratic freedoms is both well established in law[43] and increasingly a matter of concern. A topical illustration can be fund in the arrival of a law enforcement 'robot' in Singapore to disperse a group of elderly residents watching a chess match is a good example of the type of non data-related impact that is of increasing relevance in the field of police and local authority surveillance. As one of those residents was reported to have said "it all contributes to the sense… people need to watch what they say and what they do…to a far greater extent than they would in other countries[44]."

7.3 At the same time, some of the most pressing practical issues affecting the capture and retention of biometrics by every police force in England and Wales come from

---

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

[38]The International Justice and Public Safety Network, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (30 June 2011), available at https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (**PIA**) p17

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

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

[41] Activist deceived into sexual relationship with 'spy cop' wins tribunal against Met Police (telegraph.co.uk); www.bbc.co.uk/news/uk-england-nottinghamshire-58749590 accessed 3 October 2021

[42] *Wilson v Commissioner of Police for the Metropolis* [2021] UKIPTrib IPT_11_167_H In the Investigatory Powers Tribunal, para 333

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

[44] https://www.theguardian.com/world/2021/oct/06/dystopian-world-singapore-patrol-robots-stoke-fears-of-surveillance-state?; accessed 7 October 2021

confusing legislation around bail[45], the impact of voluntary attendance vs arrest and the timescales imposed for the taking of samples. These are critical matters of process driven by legislative compliance that have been raised in annual reports of the Biometrics Commissioner, none of which would be cured by data compliance. I am aware from visiting police forces that the impact of all the above issues and risks has increased since the COVID-19 pandemic[46] yet the consultation makes no acknowledgement of any of them in asking its questions for reform.

7.4 Other important areas that are not 'data protection matters' but where significant issues of public trust arise in relation to biometrics and surveillance include:

7.4.1 the police retention of images of people who have been through their custody process but have never been convicted of any offence. The national policing policy governing this widespread practice was found to be unlawful by the High Court in a case brought by two citizens[47] in 2012. Despite the ruling of Richards, LJ that "it should be clear in the circumstances that a 'reasonable further period' for revising the policy is to be measured in months, not years"[48], the arrangements to correct the situation have still not been brought into effect almost a decade later. The police hold a countless number of other such photographs, so many in fact that most police forces are unable to tell me how many they have and certainly cannot delete them using the existing functionality. The argument for their continued retention appears to be that the images are stored on databases that were built without the ability to delete them. To paraphrase the ECtHR judgment in a public protest case[49], the state cannot rely on the shortcomings of its own database to defend its unlawful retention of biometrics kept on it[50];

7.4.2 the ethical standards and practices of surveillance camera companies, some of whom have been found by Parliament to have been associated with widespread human rights abuses[51] and

7.4.3 the potential for discrimination and disproportionality in new technology for biometrics and surveillance, discrimination and disproportionality that is both intrinsic to the technology itself (in the form of algorithmic bias) or arising from the manner in which the police deploy that technology (such as the use of portable enrolment devices for fingerprinting individuals other than at a police station[52]).

---

[45] Following a separate consultation on pre-charge bail the Government has outlined the intention to legislate to remove the presumption against the use of pre-charge bail and to make it easier to use bail in cases where it is necessary and proportionate - https://www.gov.uk/government/consultations/police-powers-pre-charge-bail

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

[47] *R (On the Application of RMC & FJ) v Commissioner of Police of the Metropolis* [2012] EWHC 1681

[48] *Loc cit* at para 58

[49] *Catt v UK* App 43514/15

[50] Something which my predecessor, Prof Paul Wiles pointed out to the Commons Science & Technology Committee earlier this year - committees.parliament.uk/committee/135/science-and-technology-committee/news/156138/science-and-technology-committee-holds-followup-evidence-session-on-biometrics-and-forensics/; *accessed 5 October 2021*

[51] committees.parliament.uk/committee/78/foreign-affairs-committee/news/156425/fac-xinjiang-detention-camps-report-published-21-22/; www.gov.uk/government/publications/letter-to-baroness-williams/letter-to-baroness-williams-accessible-version; ipvm.com/reports/sanction-hikua; accessed 5 October 2021

[52] www.wired.co.uk/article/police-fingerprint-scan-uk; accessed 3 October 2021

7.5 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[53].

7.6 At the same time, there are biometrics and surveillance-related obligations on the state that go beyond data protection, obligations that may include the reliability of tools and techniques if they are to be used in a criminal investigation or prosecution. These fall within the new statutory remit of the Forensic Science Regulator[54] who is, at the time of writing, consulting on and developing his own guidance for the police and others.

7.7 The state also has *positive* human rights obligations to take practical and effective measures to protect its citizens from certain types of harm (death, torture, inhumane and degrading treatment)[55]. Often overlooked in the public debate about the use of available technology, these positive obligations would include due consideration of deploying available technology such as facial recognition surveillance cameras in the prevention of certain types of serious criminality. It is clear that this is a duty of means rather than result and the police are legally (and perhaps ethically) bound to use the means reasonably available to them[56]. The mantra of the data protection regulator is generally *"just because you can doesn't mean you should"* but, in this context, it is precisely *because* they can that the police must, if not use the biometrics and surveillance technology that is increasingly available to them, then at least *consider* those means.

7.8 And inevitably, the experience of the COVID 19 pandemic has increased public concern in this area and given rise to calls for greater vigilance and accountability in the area of surveillance[57].

7.9 Balancing these highly complex competing issues and expectations is not, on any view, simply a matter of upholding information rights and ensuring the democratically accountable use of remote biometrics, and other new technologies by the police will require more than 'data reform'.

8. Societal acceptability

8.1 In my response to the government's earlier consultation on the Surveillance Camera Code[58] I set out why I believe the future of surveillance is being shaped by what communities are prepared to tolerate and support, not just in England and Wales, but around the world. Societal acceptability here goes beyond notions of 'consent' (informed, contingent, conditional, express, implied, or otherwise) as relied upon in

[53] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
[54] See the Forensic Science Regulator Act 2021
[55] See e.g. *Valiuliané v Lithuania* 33234/07; *Rantsev v Cyprus & Russia* 25965/04; *BV v Belgium* 61030/08
[56] *Commissioner of Police of the Metropolis v DSD and Another* [2018] UKSC 11
[57]https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/
[58] www.gov.uk/government/publications/professor-fraser-sampsons-response-to-the-surveillance-camera-code-of-practice-8-september-2021 accessed 5 October 2021

the context of data protection. Acceptability in this sense is a wider democratic construct made up of ethics, mores and legitimate expectations. It may be peculiar to specific communities or generally applicable and can be seen in some of the many global reactions to technically possible and legally permissible surveillance developments such as Live Facial Recognition[59]. It can also be seen in challenges to police use of AI and automated decision-making technology in mobile phone tracking via cell-site simulators ('Stingrays")[60], Automated Licence/Number Plate Readers, Toll Payment Readers, Shot Spotters (acoustic devices), X-Ray Vans and "Surveillance-Capable Lightbulbs"[61] and the use of Open Source Intelligence (OSINT) where the relevant data protection rules are not always engaged but where the citizen's protestation tells their government that, while it may be legal, people do not want the police to do it, in their name or in their neighbourhood[62] and reports of police forces using this without being transparent about it have only served further to undermine public trust.[63] Even technophile societies such as Singaporeans are becoming alarmed at the police use of surveillance technology and stopped their law enforcement bodies using the country's COVID 19 track-and-trace capabilities[64].

8.2 Most recently, MEPs passed a resolution supporting a ban on the police and law enforcement bodies using facial recognition in public spaces and preventing their use of predictive algorithms[65]. In the United States the pressure has been greater and the democratic response by local authorities even swifter[66]. These and other examples illustrate how pressure from citizens has sought both to restrict and even *pre-empt* the use of future technological capability before the police even begin to explore its legitimate contribution.

8.3 In this way 'societal acceptability' essentially acts as a democratic brake on technological exuberance, and in the field of police biometrics and surveillance there is a marked movement towards the citizen increasingly resisting what can be done technologically and defended legally.

9. The Home Office Questions – 'Absorption' and Alternatives

9.1 Unlike the many other areas raised within the consultation, the case for 'absorption' is not made out anywhere and there are other ways of strengthening and simplifying governance (for example following the Scottish Parliament's model below).

---

[59] 4 MPS – 90% error rate (Dodd, V 2018 https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure – accessed 15 October 2021; Orlando Police Department abandoned use of Amazon Rekognition software as a result of technical issues - https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended accessed 26 August 2021

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

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

[62] www.wired.com/story/clearview-ai-new-tools-identify-you-photos/; fortune.com/2020/03/03/clearview-ai-privacy-issues/ accessed 5 October 2021

[63] New Zealand Police Trialled Facial Recognition Tech Without Clearance www.nzherald.co.nz/nz/nz-police-trialled-facial-recognition-tech-without-clearance/M6SAWXF4VK4EEZWQHMXU2XTIUI/; Audit Reveals New FR Tech Tools in Police's Digital Armoury www.nzherald.co.nz/nz/audit-reveals-new-facial-recognition-tech-tools-in-polices-digital-armoury/FR7VXHHGE4QUBFQKJ5IRXYJDJU/; accessed 9 October 2021

[64] https://www.theguardian.com/world/2021/jan/05/singapore-says-police-will-be-given-access-to-covid-19-contact-tracing-data; accessed 7 October 2021

[65] www.theparliamentmagazine.eu/news/article/meps-back-ban-on-aidriven-mass-and-indiscriminate-surveillance

[66] www.innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/

9.2 As the data protection authority for the UK, the ICO is a statutory *regulator* – perhaps the arch regulator of our time - and the reform of their functions and practices is at the heart of the consultation. By contrast the UK Biometrics Commissioner is *not* a regulator[67] and an appreciation of the functions to be soaked up is nowhere near the heart of the consultation. As discussed above, the principal functions of the Biometrics Commissioner are *quasi-judicial* in nature and are exercised in the setting of policing, counter-terrorism and national security. To characterise them as upholding information rights is to miss this fundamental point and their absorption would introduce a UK regulator to this area and then require that regulator to take on non-regulatory judicial functions. In the setting of those functions there may also be an inherent conflict for the ICO as they will find themselves participating in decisions to authorise police retention of biometrics which are later challenged by the individual who would not then be able to turn to them as the nation's regulator upholding their information rights at large.

9.3 A good description of the Biometrics Commissioner is that they *independently oversee the use of investigatory powers involving biometric material, ensuring they are used in accordance with the law and in the public interest.* But for three words this description would be identical with that of another law enforcement oversight body. The website of the Investigatory Powers Commissioner states that they "*…independently oversee the use of investigatory powers, ensuring they are used in accordance with the law and in the public interest.*"

9.4 Both the Biometrics Commissioner and the Investigatory Powers Commissioner have UK-wide roles with specific functions for national security and intrusive police surveillance including policing in Scotland and Northern Ireland, and the congruence of our statutory investigative oversight and assurance roles is striking[68]. The Investigatory Powers Commissioner's Office (IPCO) is also judicial and, to that extent, is much more readily placed to offer a simplified and intuitive alternative to the existing roles.

9.5 Given that the Biometrics Commissioner role operates exclusively within the investigative arrangements for policing, law enforcement and national security, the case for absorption (should there be one) might better be met, not by *creating* a new, non-regulatory remit for the data regulator, but by incorporating the functions into the remit of another existing judicial body with statutory responsibilities for overseeing the use of highly intrusive and sensitive tools and techniques in an operational law enforcement context. This was certainly the view expressed by my immediate predecessors in both Biometrics and Surveillance Camera roles and is one that I can see represents a far more rational transferee of those functions, albeit that some of the freedom enjoyed by holders of these offices as independent appointees (such as reporting to Parliament) might be surrendered. It should also be noted however, that in what has otherwise been recognised by the UN High Commissioner

[67] a point made repeatedly by my predecessor. See: www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019

[68] We are also both engaged in the use of sensitive personal data within policing and law enforcement.

for Human Rights office as a leading model for surveillance oversight, the UN expressed reservations[69] around the IPCO governance arrangements that require authorisation and oversight to be undertaken in the same office, a key consideration in any discussion of functional transfer.

9.6 My surveillance camera role does have a regulatory element in the context of monitoring and encouraging compliance with the Home Secretary's Surveillance Camera Code of Practice. Acknowledged by the Court of Appeal[70] as representing part of the body of law governing what is an increasingly contentious area of activity (facial recognition technology), the Code is a specialised part of the wider framework of regulation governing the lawful, proportionate and fair use of citizens' data. That framework includes statutory guidance from the Information Commissioner and the police (see the revised Management of Police Information guidance[71] currently under consultation) and may well include forthcoming statutory guidance from the Forensic Science Regulator (see above). For its part the ICO also produces guidance in this area and is developing further guidance on video surveillance at the time of writing. The Surveillance Camera Code therefore represents a series of *further principles* for the specific context of public space surveillance and is only of direct legal effect in respect of policing bodies and local authorities in England and Wales which are currently the only 'relevant authorities' designated for the purposes of the legislation[72]. The consultation does not address this aspect of the current arrangements.

9.7 So far as enforcement of the Surveillance Camera Code across England and Wales is concerned I have no powers which enable me to inspect or audit CCTV systems, enforce laws or otherwise impose a financial or other sanction - something which has been the subject of significant public debate and there have been calls by others (including my predecessor) for the government to remedy this situation[73]. To adopt the wording of the consultation, the Commissioner is able to provide advice and guidance but no redress. The ICO already has powers of redress that are deployable in some aspects of breaches of the data protection regime by the operation of surveillance cameras and, to that extent, combining the functions would bring simplification and powers of enforcement. However research into the activities of data protection authorities across all GDPR countries - including the ICO - shows a consistent *lack* of enforcement activity in the area of surveillance compliance[74] and IPVM recently found that, over the first three years of the GDPR being in place, the ICO had issued zero surveillance fines, in common with the majority of national data regulators, while only one country's data regulator - Spain - had imposed more than seven GDPR video surveillance fines over that three year period[75].

---

[69] see https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23297 accessed 2 September 2021

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

[71] Code of Practice on the Management of Police Information, issued by the College of Policing under s.39A of the Police Act 1996 to which chief police officers must also have regard.

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

[73] See the Annual Reports of the Surveillance Camera Commissioner www.gov.uk/government/collections/surveillance-camera-commissioner-annual-reports

[74] https://www.ifsecglobal.com/video-surveillance/gdpr-breaches-rife-among-cctv-deployments-investigation-suggests/

[75] ipvm.com/reports/gdpr-enforce.html accessed 5 October 2021

9.8 In discharging its broader data protection remit the ICO provides advice and guidance on all data protection-related matters and the conduct of data protection impact assessments including some that involve the use of surveillance camera technology[76] and works closely with my office; both produce guidance that is cross-referenced including the existing Surveillance Camera Code for which the ICO is also a statutory consultee[77] and the ICO was an intervener in the *Bridges* litigation arising from the police use of facial recognition capabilities[78]. In this respect there is clear potential for *streamlining* some of the arrangements for the overt use of surveillance technology by the police, but it does not necessarily follow that this would be best achieved by absorption into the ICO. Given that the primary purpose of the police use of biometrics and surveillance is to support the investigation of crime and prosecution of offenders, there is probably a more compelling argument for absorption by the *Forensic Science* Regulator than a data regulator but with the same obvious conflicts adverted to above.

9.9 Viewed purely from a data management perspective there is some logic to transferring some of the functions around the Surveillance Camera Code which is a gloss on the broader data protection guidance and advice and a transfer of this function to the ICO would reduce overlap and the number of statutory documents. However, as illustrated above, the functions of the Surveillance Camera Commissioner go beyond matters of data protection and include areas of technical standards, liaison with academia and industry, the delivery of certification schemes and working with the police and other camera operators to enable them to develop their policy and practice[79]. Further, as the proposals in the consultation apprehend a reconstituted ICO, replacing the Information Commissioner's independent appointee status, removing the independence of the Surveillance Camera Commissioner at the same time and giving functional responsibility to an *employee* of a reformed ICO would dilute some of the current advantages and safeguards.

9.10 It should be noted that the Code also applies only within England and Wales as policing is a devolved matter and absorption by the ICO of both roles would, at the very least, bring some synergies with its own existing UK-wide jurisdiction as regulator. Counter-terrorism and national security are not devolved matters and therefore the ICO's absorption of the Biometrics Commissioner's functions would fit with their existing jurisdiction for data compliance, removing the need for some parallel legislative arrangements with the Scottish government. While this might achieve the goal of simplifying the arrangements it may bring further complexities for devolution which are discussed further below.

10. Devolution issues and impact

10.1 Counter-terrorism and national security considerations for the retention and use of biometric material fall within the jurisdiction of the Biometrics Commissioner who has

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

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

[78] *Loc cit*

[79] See the National Surveillance Camera Strategy www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales

jurisdiction for National Security Determinations and associated matters in Scotland and Northern Ireland.

10.2 The Surveillance Camera Commissioner's functions cover policing and local authorities in England and Wales.

10.3 The ICO is the UK data protection authority and the regulator for national and local authorities in England, Wales, Scotland and Northern Ireland.

10.4 It is important therefore to consider the potential impact of functional absorption in relation to the remainder of the UK beyond England and Wales.

10.5 Scotland

10.5.1 The UK Parliament took a close interest in the recent policy developments in Scotland with the Commons Science & Technology Committee questioning ministers and my predecessor about the approach to principles-based legislation and public consultation on the area of legislation for "new biometrics"[80]. In the course of his review for the Scottish Parliament John Scott QC heard evidence from the ICO and, in particular, about the need for a new Biometrics Commissioner in addition to the ICO to provide specific oversight of the police use of biometrics. The ICO's response to the consultation appears to show support for the creation of the post and makes no suggestion that its absorption of these functions might be appropriate or preferable[81].

10.5.2 In response to the review, the Scottish Parliament subsequently created the role of Scottish Biometrics Commissioner in order, as explained by Justice Secretary Humza Yousaf, to "complement the work of others*, including the Information Commissioner* [my emphasis], and help maintain public confidence in how new technologies and data are being used to help keep crime down and communities safe"[82].

10.5.3 The Scottish Biometrics Commissioner, Dr Brian Plastow, was appointed on 11 March 2021, less than two weeks after my own appointment, and we have worked closely together since. He has helpfully shared his own response to the consultation with me. In his response, Dr Plastow says: "In Scotland, the approach has been to vest independent oversight in a Commissioner appointed by Her Majesty on the nomination of the Scottish Parliament. This means that the Commissioner is not answerable to, or capable of being directly influenced by Scottish Government officials or ministers. One of my functions is to develop a statutory Code of Practice on biometric data for policing and criminal justice purposes backed by powers to ensure legislative

[80] publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197006.htm

[81] The Information Commissioner's response to the Scottish Government's consultation on enhanced oversight of biometric data, 1st October 2018

[82] www.gov.scot/news/biometrics-commissioner-bill-published/

compliance. If you will forgive me for saying, I think that this has been an area of previous weakness in all jurisdictions within the UK. The absence of a specific Code of Practice for biometrics has (in my view) facilitated police 'experimentation' with certain technologies and has sometimes resulted in issues of public confidence."

10.5.4 Dr Plastow goes on to say "As these are reserved matters, I will offer no specific comment on this other than to say that debates about biometrics in policing are intrinsically complicated and linked to broader considerations of legitimacy, effectiveness and efficiency. Above all, it is about public confidence, trust, and public acceptability – so the debate is far broader than one of ensuring compliance with any prevailing UK data protection regime. In closing, I would just like to highlight that any future transfer of the England and Wales function to the ICO would also have important implications for Scotland that would necessitate DCMS consultation with the Scottish Parliament, Scottish Government, Police Scotland and the Scottish Police Authority. In particular in relation to where Scottish and UK legislation empowering the existing Commissioner independently [to] oversee biometrics retained in Scotland under national security determinations and is also as a statutory consultee in the Scottish legislation."

10.5.5 However, one immediate simplification that would flow from the ICO's absorption of the Biometrics and Surveillance Camera Commissioner's functions would come from the Information Commissioner's UK-wide jurisdiction. Under the current arrangements there is a need for the UK government to pass *additional* secondary legislation[83] to ensure that biometric data obtained in England, Wales or Northern Ireland but used by police and law enforcement bodies in Scotland, comes under the Scottish Biometrics Commissioner's functions. As the ICO already has UK-wide functions over such data the need for this secondary legislation would be obviated, thereby simplifying the regulatory framework.

10.6 Northern Ireland

10.6.1 In May 2013, the Northern Ireland Assembly passed the Criminal Justice Act (Northern Ireland) 2013, Schedule 2 to which makes provision for a new regime setting out a series of rules for the retention of DNA and fingerprints taken by police based on the seriousness of the offence, the age of the person from which the material was obtained, whether the person was convicted or not convicted and the person's criminal history. In essence this was the legislative response to the judgment in *S & Marper*[84] and is, to that extent, the equivalent of the Protection of Freedoms Act 2012. It has never been brought into effect because, according to the Justice Department's website[85], under the current provisions, *a large volume of DNA and fingerprints related to non-convicted people would fall for deletion from police databases*. To mitigate any risk that

[83] See the Scottish Biometrics Commissioner Act 2020 (Consequential Provisions) Order [Draft] 2021

[84] *Loc cit.*

[85] www.northernireland.gov.uk/news/long-anounces-consultation-biometric-proposals

the deletion of this material could undermine the investigation of unsolved Troubles-related deaths in Northern Ireland, *a form of statutory provision will be required to provide a lawful basis for deleted material to be retained and used for the purpose of legacy investigations* [my emphasis].

10.6.2 On 18 March 2020 the Justice Minister announced[86] a public consultation to alter the legislation covering the retention and use of fingerprints and DNA and "to widen the scope of the Northern Ireland Commissioner for the Retention of Biometric Material".

10.6.3 On 14 July 2021 the Secretary of State for Northern Ireland published the UK government's plans for new legislation to address the legacy of the Troubles[87] which includes proposals for a new Information Recovery Body.

10.7 Given the ICO's existing remit for data protection, the already complex landscape for oversight of information and data breaches by the police which can involve other bodies such as the Police Ombudsman[88], the proposals for a *wider* remit for Northern Ireland to have its own Biometrics Commissioner, the government's proposals for legislation to introduce a new Information Recovery Body in relation to the Troubles and the existing statutory functions of the UK Biometrics Commissioner for the retention and use of terrorism-related biometrics, it may be very challenging to achieve legislative compatibility.

11. CONCLUSION

11.1 To propose absorption of the Biometrics and Surveillance Camera Commissioner functions by the ICO is to misunderstand the realities of those functions. There is a simple logic to the proposal in the questions. The functions of the Biometrics Commissioner and Surveillance Camera Commissioner involve oversight of the use of very sensitive personal data by the police and local authorities. Closer examination of the realities and risks however, reveals some data-related functions which, if absorbed by the ICO, would almost certainly result in their receiving less attention, while there are other non data-related issues that simply do not fit with even a reformed data protection authority; if those functions are to be moved, there are far more intuitive places for them to go.

11.2 However superficially attractive some of the logic may be, it is worth reviving the wisdom of a US Supreme Court Justice[89] who said "the life of the law has not been logic; it has been experience. The felt necessities of our time."

11.3 It seems to me that the 'felt necessities' of our time very much include the need to build and maintain public trust and confidence in the police generally - which is emerging as a critical strategic imperative - and in their accountable use of biometrics

[86] *Loc cit.*
[87] www.gov.uk/government/publications/addressing-the-legacy-of-northern-irelands-past
[88] www.belfasttelegraph.co.uk/news/northern-ireland/two-suspended-psni-officers-referred-to-public-prosecution-service-as-part-of-twitter-troll-investigation-40876297.html
[89] O.W Holmes Jr.

and surveillance in particular. This probably represents one of the most pressing necessities in contemporary policing, not just in the UK but globally. The existence of an independent commissioner having specific responsibility for these areas is unusual and is seen in other countries as a statement of the importance of accountability in the police use of biometrics and surveillance. Replacing it may be seen as a statement of retraction.

11.4 Ultimately it is for government to understand and respond to the felt necessities of our time and for Parliament to consider any subsequent legislation. Some of those felt necessities in the context of invasive surveillance and the need for legislation are, at the time of writing, under close consideration by the House of Lords Justice and Home Affairs Committee[90].

11.5 Writing in the context of proposed Australian legislation, the Human Rights Law Centre noted[91] that "biometric technologies hold great potential for transforming the nature of our society – and the ordinary person's anonymity in a range of common activities, and in a range of a democratic activities. Regulation of these novel technologies, and active facilitation and development of them for collective purposes, must be informed by an educated public debate".

11.6 The consultation offers a real opportunity for an educated public debate at a time when the police face huge challenges in their use of biometrics and surveillance. We have, for example, an act of Parliament which tells the police what they must do when taking a suspect's boot print[92] but which is silent on the mass capture of facial images and other remote biometric capabilities and takes no account of frontline developments such as the increasing use of voluntary attendance over arrest, leaving the police frustrated and the public nonplussed. The need for legislative reform in the taking and matching of biometrics by the police, the challenges of bail and the 'released under investigation' status of suspects is very clear; the result is, in the words of a very experienced regional biometric manager during a recent police force visit that "we are doing a disservice to our victims and our officers"[93]. These pivotal issues should be at the centre of the consultation questions.

11.7 It is no exaggeration to say that people's lives have been irreversibly transformed by contactless biometric capabilities emerging by necessity from the exigencies of the COVID 19 pandemic and about which our communities have some profound questions of their own in the context of policing and law enforcement[94]. If the *accountable police use of biometrics and surveillance* is to be reformed, we have an opportunity to do it now, but it will take far more than the absorption offered.

---

[90] www.lawgazette.co.uk/news/invasive-police-algorithms-need-legal-safeguards-lords-hear/5110133.article; accessed 13 October 2021

[91] "The Dangers of Unregulated Biometrics Use" https://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/t/5b0cebb66d2a73781c59100f/1527574029901/Human+Rights+Law+Centre+Submission+to+PJCIS+-+Identity-Matching+Services.pdf - para 68 accessed 30 Sept 2021

[92] Police and Criminal Evidence Act 1984, s61A

[93] Visit to Derbyshire Constabulary EMSOU Forensic Science Central Services, 7 October

[94] https://www.telegraph.co.uk/news/2020/09/09/cover-covid-government-has-launched-all-out-assault-british/

11.8 The legal landscape governing data protection, privacy and the use of biometrics has been shaped less by enlightened policy planning and more by the fallout from litigation by or on behalf of the citizen and our current legal framework (including the acts that created my functions and those of the ICO) has been largely the product of legal challenge[95]. While access to effective legal remedy is itself a fundamental human right[96], the recourse to litigation is not necessarily the most efficient or effective way of asserting democratic accountability; it is certainly an expensive and unpredictable way of developing policy[97]. Contrary to views I have heard from officials during my time in post, judges should not be asked to decide matters that are essentially political, a point made by the Attorney-General only a week ago[98]. Against that background this consultation offers a rare opportunity to consider the relevant policy issues that we talk about when we talk about the accountable use of police biometrics and to design a governance framework that is a planned response to identified requirements rather than a retrospective reaction to shortcomings revealed by court judgments.

11.9 In the end, people need to be able to have trust and confidence in the *whole ecosystem of biometrics and surveillance*, which is why singling out one technological application such as live facial recognition is unhelpful and the titration of one statutory post is unimaginative. The narrow and singular proposal of absorption by the ICO is, in my view, ill-conceived; it is the wrong answer contained within the wrong question and, for the many reasons cited above, is unlikely to produce simpler, stronger governance. It is more likely to result in dilution and further complexity while at the same time squandering the chance to hear and heed what we talk about when we talk about biometrics[99]. As one of the UK's most respected authorities on terrorism and the law put it "surveillance activities of the state are growing apace and so should oversight.[100]" In terms of the specific question on absorption of functions by the data regulator, Professor Walker went on to say "I fear that the issue would be drowned in the ICO. This topic can be highly specialised but is of major importance. This fact was brought home to me by the detail that [the Biometrics Commissioner] uncovered in the national security field, including so many defects. Given that much of this activity is inaccessible to the public, it does not fit well into the ICO's remit."

11.10 It is clear that some areas of biometrics and surveillance covered by the current framework are heavily and iteratively regulated, while there are other areas such as commercial and individual private use of new surveillance technology that fall outside

---

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

[96] Art 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms

[97] See e.g. Rubin and Feeley Judicial Policy Making and Litigation Against the Government, 5 U.Pa.J.CONST.L.617 (2003)

[98] https://www.lawgazette.co.uk/law/huge-increase-in-political-litigation-braverman-defends-jr-reforms/5110211.article?utm_source=gazette_newsletter&utm_medium=email&utm_campaign=%c2%a3150k+costs+cap+rejected+%7c+Braverman+defends+JR+reforms+%7c+Law+Society+Council_10%2f20%2f2021 ; accessed 23 October 2021

[99] videosurveillance.blog.gov.uk/2021/10/12/what-we-talk-about-when-we-talk-about-biometrics/

[100] Professor Clive Walker, Emeritus Professor of Law, the University of Leeds, 2 October 2021.

any of the regulatory frameworks[101]. As I submitted to the statutory consultation on the Surveillance Camera Code this is a fast-evolving area and the evidence is elusive, but it would be a dispiriting irony if those areas left to self-determination were found to present the greatest risk to communities or simply to give rise to the greatest concern among citizens. That would be like putting all our new CCTV cameras only in places where we know someone is already watching. It may transpire that some technological surveillance capabilities such as live facial recognition are so ethically fraught, or raise such a level of discomfort from a societal perspective[102], that they can only be acceptably carried out under licence or by express authority. Any such reform would require a transformational change to the oversight regime but I believe that we need *as an irreducible minimum* a single set of clear principles by which those operating biometric and surveillance technology will be held to account, transparently and auditably.

11.11 Whether it is to be achieved by absorption or otherwise, the acid test for any reformed framework for the police use of biometric and overt surveillance technology will be how far it allows us to know that their technical capabilities (what is possible) are only being used for legitimate, authorised purposes (what is permissible) and in a way that the affected community is prepared to support (what is acceptable).

[101] See e.g. "Facial Recognition Technology: a guide for the dazed & confused", CDEI, https://cdei.blog.gov.uk/2020/06/01/facialrecognition-technology-a-guide-for-the-dazed-and-confused/ https://www.csis.org/analysis/questions-about-facial-recognition; Schneier 2020, "We're Banning Facial Recognition; We're Missing the Point" https://courses.cs.duke.edu//spring20/compsci342/netid/news/nytimes-schneierfacial.pdf; accessed 2 September 2021

[102] See for example https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3; and https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf pp. 19-28, accessed 2 September 2021