Policing, AI and the New Surveillance Relationship

Surveillance is the art of perspective. Whether siting a camera, setting an observation post or securing an entrance, the aspect from which you look will determine what you can see and, by extension, what you will miss. Crudely put, the more points of perspective you have available to you, the more complete your picture is likely to be and the less you are likely to overlook. This basic axiom can also be applied to more abstruse areas of surveillance policy and regulation but the same practical discipline is not always adopted and quite often the picture is incomplete, the view obscured or, worst of all, a blindspot is created.

While serving as the United Kingdom's first combined Biometrics and Surveillance Camera Commissioner[1] there were three particular vantage points which I found to be helpful in disentangling the competing issues and arguments. Combining the view from these three overlapping vantage positions can assist in assessing the relative weight being given by a particular position or policy or even a product[2], revealing some key issues and risks, and highlighting things that may have already happened without being spotted.

The perspectival tryptych

The three perspectives or vantage points can be adumbrated as the technologically possible (what can be done) the legally permissible (what must/must not be done) and the societally acceptable (what people support/expect to be done). Alternatively,

[1] Appointed by the Home Secretary under the Protection of Freedoms Act 2014 ss 20 and 34.
[2] As I have subsequently found as Non-Executive board member for a facial recognition company (Face Watch UK Ltd.)

they can be summarised as innovation, regulation and expectation. This chapter will consider some of the emerging features driving, constraining and reframing public surveillance by the state and will switch between the perspectives to reveal some of the key considerations, challenges and requirements of accountability in the use of increasingly intrusive technology by the police. At the same time it will consider how we arrived at the current position and what that may mean for the future and the inevitable expansion of AI-driven surveillance capabilities in policing.

Broadly speaking, the development of public space surveillance has seen the police tending to look towards their legal powers, the commercial sector the technical functions and the citizen on the Clapham omnibus[3] fixedly staring at the screen of their mobile device while the changing street scene passes unnoticed outside the window. In many different forums including a regular online column[4], have encouraged each group to consider the situation from all three perspectives before taking a position on a particular question or issue. The three perspectives are not by any means discrete and overlap considerably. Innovation, for example, has changed surveillance behaviour of both the state and the citizen. Look for example at the first thing that most police forces now do when faced with a significant incident or occurance. The police response - not just in the UK but in many jurisdictions – is to issue a public request for the citizen to share images from their personal devices which might include anything from GoPros, doorbells, dashcams, shedcams. Why do they do this? Because someone almost certainly captured something relevant to

[3] This is the fictional reasonable member of the public, suggested by Collins MR in *McQuire v Western Morning News* [1903] 2 KB [100], [109]. The metaphor persists and that person can now also be found on the "Bondi tram" in Australia: *Steinmetz v Shannon* (2019) 99 NSWLR 687, [44].

[4] Fraser Sampson, 'Remote Biometric Surveillance and Policing - A New Frame of Reference' *Biometricupdate* 27 August 2024 https://www.biometricupdate.com/202408/remote-biometric-surveillance-and-policing-a-new-frame-of-reference

the investigation. This phenomenon has recently manifested itself in police forces asking the citizen *not* to share their images and recordings of an event in a public space[5], illustrating both the evolving inter-relationship between the citzen *qua* surveillance agent and the state, and also the extent to which the police feel authorised (or even obliged) to intervene in private message sharing. The reason behind this significant interpositioning between the police and the citizen is two-fold. First, because we as a society are capturing more and more images and recordings of every aspect of our lives (the societal), and seconly becausetechnological availability (the possible) has enabled us to do this beIn terms of the available technology the citizen in many (arguably all) jurisdictions around the globe is now empowered with extraordinarily potent surveillance capabilities. We can go online and buy sunglasses with built-in camera and live messaging capability, acquire a drone and pilot it from our mobile phone or use our doorbell to see who is at the door, not just from another room but from the other side of world. As I reported to parliament[6] this is surveillance capability that only recently was the preserve of state intelligence agencies.

This significant development has been produced by a combination of technological capability and societal evolution; acknowledgement of how this has changed also requires recognition of *the speed* at which it has done so. At the same time, AI-driven capability is itself changing at redshift speed and will be increasingly challenging to track. The expansion of social media and its parallel preoccupation

---

[5] Libby Brooks, 'Police ask public not to share images of man in fatal bus collision in Edinburgh' *The Guardian* (London, 3 November 2024) https://www.theguardian.com/uk-news/2024/nov/03/police-ask-public-not-to-share-images-of-man-in-fatal-bus-collision-in-edinburgh

[6] [United Kingdom] Commissioner for the Retention and Use of Biometric Material, *Annual Report 2021-22* (2002) para 103 <https://assets.publishing.service.gov.uk/media/63e3ce2fd3bf7f17347092c4/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf>

with self-surveillance has resulted in a situation where an increasing amount material on which policing relies is no longer coming from 'official' cameras on lampposts and vehicles; it is coming from *the citizen*. Changes in technology-centred lifestyle mean that many Western states are now shifting from a history of surveillance which relied on images *of* the citizen to one which will depend on images *from* the citizen. This elemental shift – remisicent of China's digitally revived Sharp Eyes strategy[7] – is very significant, not only technologically and societally but legally as will be discussed below.

Closed circuit surveillance

An example of how all three lenses of perspective can come together may help to illustrate their relevance and interoperability. Decades of investigating the impact that public space CCTV may have on crime has been voluminous, energetic and inconclusive[8] but the relevance of traditional closed circuit television cameras for the future of surveillance is now questionable for a number of reasons. Applying the perspectival tryptych, technologically all the established research into the subject was undertaken when public space surveillance cameras just captured images. Surveillance devices are now much more than 'cameras', with most being smart devices capable of of many functions, one very basic of which is to take a picture. Many devices are networked computers that are not on closed circuits and certianly not on 'televison'. The AI- driven device knows it is looking for me, it knows what I

[7] That strategy is summarised in Dave Gershgorn, 'China's "Sharp Eyes" Program Aims to Surveil 100% of Public Space' (3 March 2021) https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/ The overall effect of the strategy has been described as an 'Orwellian nightmare' that will see Chinese law enforcement agencies 'matching video images, social media activity, online purchases, travel records and personal identity into a "police cloud" that is a fully integrated database: W Garrett 'The Dark Side of Artificial Intelligence: Challenges for the Legal System' in Judicial Commission of New South Wales, *Handbook for Judicial Officers* (2021).

[8] The research is helpfully summarised here: Phillips, Coretta. 'A review of CCTV evaluations: Crime reduction effects and attitudes towards its use.' *Crime prevention studies* 10.1 (1999): 123-155.

look like, sound like, how I walk, what I wear and drive – not just 'on the night in question' but generally. The smart surveillance device knows where I have been, where I am going, when and with whom – again, not just at the time in question but habitually. It can teach other devices and learn from them, it can retrieve, combine, recall, synthesise and share information; it can communicate. Every time it looks for me the smart surveillance device gets better at finding everyone. Societally, I, the person being sought, know all this too and it is a reasonable hypothesis that these features ought to have some direct impact on offending – even if only mine - in a way that CCTV could not have been expected to do. As a citizen I am now as familiar with some tools of surveillance as an intelligence operative from the Cold War era and if I am unsure how to use and misuse them, world class know-how and 'as a service' support are only a mouse click away. This is an entirely different situation from that of monolithic CCTV infrastructure and the static grainy images it produced. The legal perspective reveals how the regulatory infrastructure in many jurisdictions grew up around CCTV and privacy considerations making provision for a wholly different technological and societal era than now obtains. This is particularly clear in the UK where there is a statutory surveillance camera code of practice[9] which covers the overt operation of cameras by the police and local authorities but in public spaces. While it makes some provision fort he use of Live Facial Recognition surveillance systems by the police, the Code says nothing about the sharing, retention and use of citizen-generated public space surveillance images or other data. Contrast this with the decision at the time of writing in August 2024 of the New South Wales government to unveil its innovative BluLink tool which will allow citizens

[9] 'Surveillance Camera Code of Practice' Home Office, first published June 2013 and amended November 2021 and March 2022 https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

calling the national emergency number to upload data and livestream footage of events direct to the police[10]. As the ministerial press release stated this technology will give the police access to the scene before they have even arrived. Direct video feeds from the citizen-on-scene are the next development in the new surveillance relationship described at the start of this chapter and will bring different challenges from those of descriptive reporting of crimes. Legal considerations of agency, direction and control will arise, as will personal matters of disclosure and identification and the need for protection in the prosecutorial process[11]. None of these issues are directly covered by the current regulatory regime in the UK and the surveillance camera code does not cover citizen-generated data sharing[12]. In short, rapidly evolving technology is being habitually used by the citizen to such an extent that the state is increasingly reliant upon citizen-generated data captures, while the regulatory framework, created for and in a pre-AI era when public spaces were watched over by one-dimensional image capture devices from fixed points, continues to focus narrowly on those systems operated by local policing and government bodies[13]. Even a brief comparative review of CCTV literature and regulation against communication and data sharing cultural norms reveals a stark dissonance between what can be done, what is being done and what the state says must or must not be done in public space surveillance.

---

10 https://www.police.nsw.gov.au/news/news_article?sq_content_src=%2BdXJsPWh0dHBzOi8vZWJpenByZC5wb2xpY2UubnN3Lmdvdi5hdS9tZWRpYS8xMTM3MzAuaHRtbCZhbGw9MQ==

11 See e.g. *R v Hewitt and Davis* (1992) 95 Cr.App.R 81; *R v Grimes* [1994] CLR 213 where the courts considered the legal situation of householders who allowed the police to use their premises as vantage points from which to conduct surveillance of suspects. It was accepted that citizens who do so are essentially in the same legal position as informers and therefore exposed to the same risks of identification and recrimination. How far this line of thinking will – or even can – be extended to the citizen *qua* surveillance agent remains to be seen.

12 https://www.gov.uk/government/publications/update-to-surveillance-camera-code

13 Surveillance Camera Code of Practice *loc cit*

Applying a perspectival tryptych can thus combine to create a richer, clearer image of what is already happening around us but which we may have missed. It can also help to understand frustrations, paradoxes and contradictory positions which will be considered below. Failing to take all three perspectives into account or over emphasising one without regard to the others can create problems. An example can be found in the early policing experimentation with AI-driven capabilities in several Western jurisdictions. In a development of a push towards actuarial policing where crime is purportedly pre-empted[14], pioneering police forces sought the support of algorithms to calculate future crimes as an expansion of existing data analysis and current practices. The result was police organisations taking algorithms that were originally designed to predict aftershocks from earthquakes and using them to predict street robbery[15]. There is, of course, a profound irony in purporting to use seismic aftershock predictors in this way without predicting consonant aftershocks to public trust and confidence but the episode is cited here primarily to illustrate what can happen when one or more perspectives is partially obscured or a complete blindspot.

When Facial Recognition Technology (FRT) began to offer the state a new aspect for remote biometric surveillance a similar assymetry emerged. From the somewhat unusual legal perspective in England and Wales, policing enjoyed not only the general powers to take photographs in the traditional sense, but also an express - albeit very limited - stautory authority that supported its use of public space

[14] See e.g. https://biologicalsciences.uchicago.edu/news/algorithm-predicts-crime-police-bias
[15] https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/; https://www.vice.com/en/article/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed/

surveillance systems (along with those of local authorities)[16]. This permissive regulatory environment allowed the experimental use of live FRT by the police, generating significant controversy and attracting formal legal challenge[17]. Little policy and legislative attention was given to some of the broader legal implications[18] or the societal expectations or sensibilities of the population. When the police use of live FRT was successfully challenged[19], the legal position as set out by the Court of Appeal was widely misunderstood by many stakeholders, including ministers with responsibility for policing and was cited by Matthew Ryder KC in his independent review of biometric data governance in England and Wales[20]. Technologically, the early algorithms were challenged on the basis of 'inherent bias' when scanning faces of people with darker skin tones and/or women[21] and the fact that the police had not provided sufficient performance data for their algorithms to disavow suspicions of 'bias' or, more properly, the production of uneven results when used to match faces of people having certain characteristics. While the principal police force pioneering the use of FRT, the Metropolitan Police Service, subsequently commissioned and published a report from the National Physical Laboratory[22], those opposed to the use of FRT by policing continue to cite historical data as evidence on inequality[23]. As I have recorded elsewhere[24], a decade is an aeon in biometric technology and bearding police chiefs with such historical statistics is jousting with fossils.

---

[16] Surveillance Camera Code of Practice *loc cit*
[17] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA 1058.
[18] Such as the Equality Act 2010 and European Convention on Human Rights
[19] *Bridges loc cit*
[20] 'The Ryder Review – Independent Legal Review of the Governance of Biometric Data in England and Wales', (The Ada Lovelace Institute, 29 June 2022) https://www.adalovelaceinstitute.org/project/ryder-review-biometrics/
[21] REF
[22] Xxxx which found that xxxxx
[23]
[24] Fraser Sampson 'Policing and facial recognition: what's stopping them?' *Biometricupdate* 16 October 2024 https://www.biometricupdate.com/202410/policing-and-facial-recognition-whats-stopping-them

Moreover, even where a clear and specific express power to take the original image of a citizen has been used, the continued retention of that image by the police once the power has lapsed has been ruled unlawful[25] in England and Wales. The national policy for retention of such images having been rule unlawful, the court directed the police that it should be clear in all the circumstances that a 'reasonable further period' for revising their retention policy was 'to be measured in months, not years'[26]. At the time of writing the police have nevertheless failed to delete large numbers of unlawfully held images of citizens who have no criminal convictions. The Home Office have been unable to say how many such images are held but it is believed to be in the millions and some of those images have subsequently found their way onto police FRT watchlists (Radiya-Dixit 2022). The police answer to this has been a plea to the technologically possible, arguing that their database does not have the bulk deletion capability necessary to comply with the court's order. Not only is this defence unacceptable from the societal perspective[27], it is also unsound legally[28].

Just because they can?

A key consideration when approaching the technological, legal and societal issues in the context of policing is the differences between the obligations and powers of the police *vis-a-vis* those of any other surveillance setting.

[25] *R (on the application of RMC and FJ) v Commissioner of Police for the Metropolis & Ors* [2012] EWHC 1681 Admin.
[26] *Loc cit* (Richards LJ) [58].
[27] https://www.theregister.com/2018/05/25/ukgovs_mass_collection_of_custody_images_is_unacceptable_say_mps/ [accessed 9 Nov 2023]
[28] *Catt v UK* application number 43514/15 European Court of Human Rights

When explaining the rationale behind a regulatory regime for technological innovation, data and privacy regulators like to say: “just because you can doesn’t mean you must”. While this may be the case for data protection and privacy regulation of individual and commercial use, the axiom is not necessarily applicable in law enforcement. The police in England and Wales have a duty to protect the citizen from certain types of harm[29] using ‘means’ that are readily available to them. It seems highly likely that those ‘means’ will include (now or at some point in the near future) proven technological capability such as AI-driven surveillance. In addition, the public expect the police to use technology when investigating or preventing certain types of offence[30]. Engaging all three perspectives, this issue suggests that, in policing, what can be done, sometimes means it must be done because the law dictates it and the citizen may expect it.

Against this backdrop of possibility, obligation and expectation, one might expect the adoption of AI-driven surveillance capability such as FRT to have been much more widespread and rapid than has happened thus far. A surveillance and AI question often raised by the police and ministers (less rhetorically than pragmatically) is “what is stopping us?” The triptych may supply, if not the answer, then at least some evidence from which some hypotheses may be distilled.

Doing nothing wrong

Adopting a legal perspective and pointing to their statutory or common law powers to capture images and biometrics, the police in the UK have consistently maintained

[29] *Commissioner of Police of the Metropolis v DSD and Another* [2018] UKSC 11 – positive obligation to investigate breaches of behaviour contravening Art 3 European Convention on Huma Rights extends to proper operational inquiry using available means.

[30] https://pds.police.uk/national-policing-digital-strategy-2020/national-policing-digital-strategy-2020-2030/the-big-picture/

that they are doing 'nothing wrong' in deploying what they regard as digital extensions to existing practices. This view is often reinforced by reference to a long-held (yet wholly fallacious) argument in law enforcement that 'if you've done nothing wrong you've nothing to worry about'. The literature on intrusive surveillance debunks this approach which says only the guilty need worry (see e.g. Joern, 2009; Anderson *et al*, 2018) yet it is still frequently deployed by the state[31]. In the context of police surveillance and remote biometrics this engrained belief endures. For example, when addressing the Royal United Services Institute in 2020, the UK's most senior police officer at the time, Dame Cressida Dick, said:

> In an age of Twitter and Instagram and Facebook, concern about my image and that of my fellow law-abiding citizens passing through LFR [live facial recognition] and not being stored, feels much, much, much smaller than my and the public's vital expectation to be kept safe from a knife through the chest.[32]

The lingering presence of the fallacy is corroborated by Dame Cressida's reference to 'fellow law-abiding citizens' which is deployed as part of a wider 'security vs privacy trade-off' (Solove 2020). While reflecting the very narrow statutory position that if the police are empowered to use the technology they are, to that extent, doing 'nothing wrong' themselves – the fallacy can be seen to be fundamentally flawed from a wider legal perspective of surveillance[33]. As it presents such a significant obstruction to the societal acceptance of the police use of AI-driven capabilities in

---

[31] https://hansard.parliament.uk/Commons/2020-06-24/debates/062FA715-C506-4F43-9F2B-0DBDF51331C3/WestferryPrintworksDevelopment; Home Secretary Wants to Restrict Use of Tents by Homeless 5 November 2023 https://www.bbc.com/news/uk-67321319

[32] Speech of Dame Cressida Dick to RUSI Financial Times 25 February 202 https://www.ft.com/content/a1228984-5713-11ea-a528-dd0f971febbc [accessed 7 November 2023]

[33] https://www.amnesty.org/en/latest/campaigns/2015/04/7-reasons-why-ive-got-nothing-to-hide-is-the-wrong-response-to-mass-surveillance/

the future, I published a deconstruction of it in advance of giving evidence to parliament[34]. That deconstruction[35] can be summarised in this way:

1. **Presumption of Guilt.** The *citizen* must prove they have 'done nothing wrong', reversing constitutional safeguards of the presumption of innocence. The fallacy allows the State to transfer the burden of proof to the citizen against a clear inference that privacy, freedom of movement, speech etc. are only enjoyed at the pleasure of the State rather than as universal rights. Moreover, it puts the individual in the notoriously difficult position of having to prove a negative.
2. **(a) Database infallibility (computer says "wrong")**. Deference to a database or algorithm means that, if the computer says the citizen has done something wrong, then, as a matter of record, they have 'done something wrong'. If the computer is a device operated by the police looking for indicia of criminality, the irresistible inference is that the citizen identified is also *prima facie* a criminal. Faced with having to prove a negative (see Reason 1) the citizen now has the exponentially harder task of disproving the entries on the police database.
3. **(b) Database fallibility (computer *is* wrong)**. Sometimes *the computer* has 'done something wrong' and people judged by algorithms often have to meet a standard far higher than the algorithm was itself. Confusing precision with reliability, this means the citizen must go beyond simply proving their innocence by disproving an entry on the police watchlist database (Reasons 1& 2(a)) and must now *discredit* the system itself.
4. **Accept or admit**. The argument imposes a false dichotomy then assumes the answer. It also assumes benignity in all State intrusion. Once it has been determined that the citizen has 'done something wrong' by way of a flawed criminal prosecution relying on the algorithmic records, the best tactical option at trial (even as someone who has not done anything wrong) may nevertheless be fort hem to plead guilty. Admitting culpability the citizen thus vindicates the premise itself, adding insult to ignominy[1].
5. **Appeal to innocence**. Opposing the argument is regarded culturally by the police as self-incriminating: resisting it supplies the corroborative evidence of 'wrongdoing' (in the same way as when the citizen requests a lawyer right after being told they are entitled to one).
6. **Done nothing wrong?** What does the state mean by 'wrong'? Speeding? Absenteesim from work? Breaching the COVID-19 lockdown rules?

Humanity errs and the fallacy leaves no one capable of being consoled by absolute innocence. Rules change after technology and things that were not 'wrong' when surveillance systems were approved may become so.

[34] Evidence of Prof Fraser Sampson to the Joint Parliamentary Committee on Human Rights, 22 February 2023 https://committees.parliament.uk/event/17397/formal-meeting-oral-evidence-session/ [accessed 6 Nov 2023)
[35] https://videosurveillance.blog.gov.uk/2021/05/27/if-youve-done-nothing-wrong-5-reasons-why-this-is-no-defence-for-surveillance/

The ‘done nothing wrong’ fallacy is compounded by a paradox for policing. As seen *supra* the citizen is enthusiastically surrendering sensitive personal data and now deploying intrusive surveillance technology such as smart doorbells and IoT devices, sharing it not only with private companies but also with the police themselves. Innovative and affordable technology (the possible) is being used by the citizen routinely sharing sensitive personal data and facial images with private companies in financial, retail, travel and security sectors with alacrity (Steinacker *et al*, 2020) and sharing personal datasets and images with the police (the acceptable)[36] while the law not only permits the use of reasonable and available means to protect the citizen from serious harms, but mandates it. Does that mean the state may presume, as Dame Cressida did, that the citizen would not only support the police using FRT in order to protect them from serious harm but would also *expect* that they would do so? For the citizen to embrace technology so enthusiastically of their own volition and at their own expense when tracking their own property, monitoring their children and visitors at their front door in pursuit of the same specific outcomes (safety and security) which are part of the overall strategic responsibilities already being undertaken by law enforcement, but at the same time oppose the police doing so would seem *prima facie* paradoxical. However, the broader societal perspective reveals a number of features relating to adoption of technology and acceptance when data sharing by the citizen. First, there is a well-established concept in online behavioural studies which broadly states that domain-specific privacy concerns do not sufficiently explain domain-specific privacy behaviour (Brown, 2001). While undeveloped, the concept – known as the privacy paradox - as originally proposed

[36] https://www.theguardian.com/world/2023/sep/07/uk-owners-of-smart-home-devices-being-asked-for-swathes-of-personal-data [accessed 7 Nov 2023].

has found empirical support (see e.g. Dienlin & Trepte, 2014). Observed online behaviour of customers and attitudes to biometric technology has also been recognised as a practical challenge in the financial technology sector, revealing a divergence between what customers believe about gaps or risks in security and their subsequent activity in spite of that belief (Rádulescu, 2018). Second, insofar as policing and state activity are concerned, research shows how public attitudes to the police use of FRT and other remote biometric surveillance capability are ambivalent (see e.g. Ezzeddine *et al*, 2023) and that the citizen is reportedly increasingly uncomfortable with, and even resistant to, the use of some new forms of intrusive surveillance technology by the state[37]. Add to that the early experimentation with new technology such as facial algorithms and continuing issues such as serious police data breaches[38] and an assumption of support is much harder to corroborate. Failing to take these societal and legal issues into account, while at the same time relying on a flawed presumption that unless the citizen is guilty of some undefined wrongdoing they have nothing to fear from intrusive technology, the police risk frustrating the adoption of evolving technology such as FRT and other AI-enabled capabilities.

---

[37] See e.g. Ada Lovelace Institute: Beyond face value: public attitudes to facial recognition technology, September 2019 Report.

[38] https://www.bbc.com/news/uk-northern-ireland-66578582. https://www.politico.eu/article/crime-victims-details-accidentally-included-in-police-foi-responses/. https://www.theguardian.com/uk-news/2023/aug/26/met-police-on-high-alert-after-it-system-holding-officers-details-hacked. https://news.sky.com/story/south-yorkshire-police-loses-nearly-three-years-worth-of-body-cam-footage-with-an-estimated-69-cases-affected-12945797. [Accessed 1 September 2024]

Surveillance partnerships

In his valedictory report as HM Chief Inspector of Consabulary for England and Wales Sir Tom Winsor said[39] policing needs "a material intensification of partnership with the private sector - that is soundly and enduringly based on trust and common interest." Nowhere is that need likely to be more evident than in biometric surveillance.

As has been shown supra, the changing technology-driven behaviour of both citizen and police has already created new dependencies and new evolutionary partnerships for public space surveillance. So far this has been confined to the sharing of images and personal data but the trend is moving towards other biometrics. For example, a leading UK supermarket has reportedly begun to issue DNA kits to its delivery drivers in response to an increase in spitting[40] so that the DNA sample may be used to create a profile by the police investigating the matter. In this way the 'act of collection' (Klosowski 2020) traditionally undertaken by the police exercising legal powers becomes blurred and the ongoing data association that links the citizen to the investigating body is freighted with unique policy considerations and legal consequences. A scenario where privately made voice recordings are shared and analysed for investigative or intelligence purposes is easy to imagine and direct livestreaming to the police of privately captured activities by citizens and businesses may soon become *de rigeur*. It will become harder for the citizen and the police to differentiate between sources of digital information but the more the state *can* do with technology, the more important it will be for agencies

[39] https://assets-hmicfrs.justiceinspectorates.gov.uk/uploads/State-of-policing-2021-1-single-page.pdf page 60
[40] https://www.telegraph.co.uk/business/2024/08/16/tesco-gives-delivery-drivers-dna-tests-abusive-customers/#:~:text=Tesco%20has%20armed%20its%20delivery,on%20assaults%20on%20staff...

such as the police to show what they are *not* doing with it if they are to retain accountability and public trust.

As the preponderance of technological capability control migrates to private companies and systems operators, questions of access and storage will arise, particularly where there is a recurring revenue requirement for software licences and upgrades. Winsor's predicted requirement for trusted partnership will also have societal as well as legal implications for ethical procurement and the police will need to pay closer attention to the trading history of surveillance partners and be more aware of the company they keep[41]. Further, experience has shown how 'use case' expansion (also known as function creep) which has been shown to increase with synchronisation of State functions and databases (Koops, 2021) and particular vigilance will be needed in this aspect of surveillance. Issues of consent and authority will arise and, while contractual arrangements between the commercial provider and the citizen are pre-eminent in technology service provision, little if anything in the relationship between the citizen and the state relies on express consent. The broader issue of consent generally is also a very significant one within the General Data Protection Regulation (GDPR) framework for data processing[42] in which, even in non-law enforcement settings, the use of FRT is so potentially intrusive that nothing short of express informed and freely given consent will make its use lawful[43]. The ability to choose or even influence the surveillance relationship

[41] https://hansard.parliament.uk/commons/2022-11-24/debates/22112428000007/SecurityUpdateOnSurveillanceEquipment; https://findbiometrics.com/uk-police-plagued-by-digital-asbestos-identity-news-digest/

[42] https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/

[43] See Office of the Information Commissioner UK guidance https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/#when5 [accessed 9 November 2023]

with the state is also very different in a commercial setting. Where there are some basic ways that consumers can react to what they perceive as privacy invasions (Poddar *et al*. 2019) like opting out or *strategically managing* the information they choose to share with commercial entities, the interrelationship between the citizen and the police is wholly (and arguably uniquely) distinct from any other founded on a digital nexus. The citizen's relationship with the state cannot be seen in terms of the "economic exchange" between data processor and "consumer" which is the context for much research in this area (see e.g. Motivalla & Li 2016) and the implications of commercial databases being used as proxies for the investigative, intelligence-gathering and prosecutorial purposes of the state need further investigation.

Conclusion

I have heard arguments from the police and government officials that FRT is simply a logical, digital extension of the police power to take pictures, but facial recognition is no more "just" photography than DNA profiling is "just" chemistry. British policing has a history of successful adoption of sophisticated and novel biometric technology (e.g. breathalysers, DNA profiling, TASER) and deploying it accountably and proportionately in the interests of a more effective operational response to emerging threats while balancing its use against the wider fundamental rights of the citizen. But it did not achieve this by pretence that there was nothing new to see and that only the guilty need be concerned. In global terms, innovation in surveillance technology has enabled the capture, editing, synthesising and analysis of images previously unaccessible to, and unusable by law enforcement bodies. Wider AI-driven remote biometric surveillance technology using voice analytics, gait

comparison and every other form of life in what might be described as *zoemetrics*[44] is rapidly becoming accessible to all. At the same time, innovation and expectation have reordered the surveillance ecosystem and the co-dependencies on which it is founded. Unlike the often imagined dystopian scenarios, public space surveillance is no longer about how many cameras the police have and where they put them; it is about what they can now do with the data from everyone's cameras (and phones and other devices). From a societal perspective the citizen is experiencing a seismic shift in status from being the object of state surveillance apparatus to a key component in its effective operation, while the law by which all is governed has remained largely unmoved. In future the state will rely less on a surveillance infrastucture comprised of its own devices and operators and instead depend on the product of the aggregated surveillance capability of their communities working in partnership. In democracies governed by the rule of law that will require recognition of the nascent digital surveillance relationship between the citizen, the state and the technology sector. Litigation enforcing state access to privately held databases and material has highlighted some of the issues (Sampson 2016) but is unlikely to inculcate the trust and confidence that this new world will need. A principles-based approach to a techology-agnostic regulatory framework such as can be seen in the EU AI Act[45] and data regulators' codes[46] will be needed, not simply for regulation, but for avenues of wider accountability in the use of AI by policing[47].

---

[44] Annual Report of the Biometrics and Surveillance Camera Commissioner 2021/2022 laid before Parliament Feb 2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

[45] https://artificialintelligenceact.eu/

[46] See e.g. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/; https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf; https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[47] https://www.ap4ai.eu/

The fundamental changes set out in this chapter are revealed by the perspectival approach, enhancing the relevant features and exposing the assymetry in the weight being given to, or assumed from, any one perspective. Any viable policy framework will need to recognise and reckon with these realities of policing, AI and the new surveillance relationship.

References

Sampson, F., (2016) *"Whatever You Say…The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation."* in Policing: A Journal of Policy and Practice, Oxford University Press, 2016 Vol 10 Issue 3 pp 222-231.