# Using Automated Facial Recognition Technology in Britain

**Mike Nellis**

**Introduction**

Developments in artificial intelligence (AI) over the past two decades (AI) (especially the combination of deep learning, more complex algorithms and the ethically dubious practice of harvesting vast online datasets of images on which to train them) have finally made a cluster of automated facial analysis and facial recognition technologies commercially viable in a variety of contexts, including law enforcement (Hare 2019). Amazon, Microsoft, IBM and Megvii/Face ++ (a Chinese company) are key players, but a US-compiled index estimates that 127 automated facial recognition (AFR) algorithms, many in smaller start-ups, are now on the market (cited in Fussey and Murray 2019:21). The availability of ostensibly reliable equipment, a wider political economy of accelerating automation, smart environments and organisational aspirations to "better than human" performance levels, underpins the surge in police deployment of AFR around the world – 64 countries, Britain included - invariably with some degrees of controversy in liberal democracies, less or none in more repressive states (Feldstein 2019).

Potentially the advent of AFR represents a significant intensification of visual surveillance in public spaces, including the capabilities, if needed, to track a person of interest as they move around a city, and to pick a face from a crowd or a queue in a street, square stadium or border checkpoint. Precisely because it can entail the mass scanning of law-abiding citizens' faces without their direct consent in order to find a match with a suspect, "live" AFR seems inherently more invasive of privacy that conventional public space CCTV systems, whatever protocols may be designed-in to manage or discard superfluous images. AFR's routinised use in China's urban public spaces, alongside ubiquitous internet and phone surveillance, all managed by AI, has already imbued it with sinister connotations (Strittmatter 2019), all the more so as China exports AI and AFR, and an associated "security model", to 63 other countries, with one company, Huawei, responsible for at least 50 of them (Feldstein 2019). While the pace of deployment in the West is not on the same scale as China, and the purposes currently more limited, government collusion with market-driven developments in liberal democracies pose new challenges, which do need to be faced.

This article will outline the institutional milieu in which AFR technology has been developing in Britain under a Conservative government, concentrating on England and Wales, but mentioning Scotland, where the situation is different, only towards the end. England and Wales has devised no specific legislation or official policy on facial recognition, although inferences could conceivably be drawn from existing laws relating to other biometric practices. Only three police forces (out of 43) have used it so far, alongside an unknown number of private companies which own and manage public space (residential complexes, shopping malls, music and conference venues). This has the tacit approval of the Home Office (the government ministry responsible for policing), but provokes the ire of civil libertarian pressure groups, notably Big Brother Watch (politically centre right) and Liberty (liberal left), the Liberal Democrat political party (a keen champion of civil liberties), *The Guardian* (a liberal newspaper) and *The Register* (an online bulletin with a critical eye on tech developments). Liberty, following the recent example of several US cities, wants to ban the use of AFR. It supported a British court case challenging it's legal basis in one particular police force, which it lost, although an appeal result is pending (February 2020).

While the Home Office's attitude towards the deployment of AFR is somewhat lax, England and Wales's three independent, state-appointed commissioners charged (respectively) with enforcing, encouraging and advising on particular fields of data management - the Information Commissioner (data protection), the Surveillance Camera Commissioner (CCTV, Speed Cameras and Automated Number Plate Recognition (ANPR) systems) and the Biometrics Commissioner (fingerprint and DNA databases) - have each expressed serious concern about the government's seemingly wilful refusal to create a clear regulatory framework for current and future practice.

**The Technology and its Critics**

Automated facial recognition (AFR) software maps the unique biometric ratios between a person's facial features (typically, but not only, eyes, nose and mouth) and converts them into "digital signature" which can then be read by an algorithm trained and capable of constant improvement (by exposure to vast databases of faces) to match these signatures. It can be an effective verification technology at automated passport checkpoints, or as a means of securely accessing one's smartphone. It can be used to match photographic or video evidence against a database ("watchlist") of known individuals and it can be used "live", in real-time to match faces in crowds, streets and stadia to such databases, albeit in less optimal conditions. It can keep track of a known or unknown person of interest as they move from place to place in a city. It can be used separately or in tandem with existing CCTV systems (albeit with different cameras) in multiple locations, with "watchlists" of varying size, quality and comprehensiveness.

AFR – and related facial analysis technologies – are not the sole preserve of policing and border security. Retailers have used facial biometrics to recognise and track particular individuals as they move through a store or shopping centre to monitor their engagement and purchasing patterns, without necessarily needing to know who they are, or matching them to a database. Sophisticated forms of facial *analysis* software – HireVue, and Amazon's Rekognition, for example - can register signs of seven allegedly "universal" emotions in facial micro-expressions - happiness, sadness, disgust, anger, surprise, confusion and calmness – sometimes augmented by voice analysis, and may have uses both in retail and staff recruitment, as well as "deception detection" at borders. *The Economist (9.9.17)*, a business magazine surprisingly alarmed by AFR – "Facial recognition is not just another technology: it will change society" - has reported research claiming that facial analysis can systematically identify men's sexual orientation (women's less so). The researchers aim was expressly not to encourage this, but to demonstrate its possibility, and to highlight the obvious dangers of it in regimes where homosexual acts remain despised and/or illegal.

AFR is already caught up in formulaic debates about security and liberty, the so-called necessary trade-off between privacy and safety which besets all surveillance technologies. Its champions insist that it is a vital new and cost-efficient policing tool, while presenting it as a *mere* refinement of CCTV, or *just another* biometric, akin to fingerprinting in order to reassure a perhaps sceptical public (which underplays the constitutive role of AI within it). They assume in times of insecurity that arguments from necessity and proportionality will always be on their side. Critics point out the mass scanning and (brief) recording of many faces subjects unwitting citizens to "a virtual identity parade" (Kaltheuner 2020). Unlike other widely used biometrics, DNA testing and fingerprinting, faces can be registered at a distance, without bodily contact or the subject's conscious awareness, making them easier to record and store without a subject's consent or knowledge. (Gait recognition, the other at-a-distance biometric, is not commonplace). Critics have further argued that outside the laboratory, in real-world conditions (constant motion, poor lines of

camera sight, variable lighting and adverse weather conditions) the technology is inherently inaccurate, generating an excess of false positives and false negatives, risking false arrest and unsafe convictions. Major manufacturers AFR software has also proven discriminatory in terms of race and gender: an MIT study has been repeatedly cited by critics to highlight AFR's persistent misrecognition of darker skinned faces, Black women most of all (Buolamwini and Timmit 2018). This should indeed constrain deployment now, but ironing out such software flaws, via better training of algorithms, (unless a pernicious authority wants them retained or even designed-in), is both feasible and likely, but the implications of *perfected, non-discriminatory*, facial recognition are arguably even more ominous.

Some of the nascent public concern about AFR reflects the secrecy with which tech companies and police forces, in the absence of clear regulatory frameworks, have developed their systems. How large are the watchlists used by the police? How long are faces kept on them? Can they be removed? Do the police trawl crowds to find and add new faces? In the US, Clearview AI scraped Facebook and other social media sites without consent to build a vast database – reportedly 3bn - of labelled faces, for the purpose of improving algorithmic recognition (Hill 2020). Anxieties about the uniquely intrusive potential of AFR has led three US cities (and some music festivals) to ban the scanning of live video feeds for suspects' faces, starting with San Francisco, followed by Oakland, and Somerville in Massachussets (Schneier 2020). Here in Britain, Liberty has called for a complete ban too.

That is unlikely to happen. Three police forces in England and Wales have trialled AFR since 2014 – Leicester, The Metropolitan Police ("The Met" – covering London) and South Wales, all using the NeoFace Watch system from Japanese company, NEC. Leicester piloted the tech for six months in 2014, but used it only once, at an international music festival in Donnington in 2015 (with some facial images from Europol on its watchlist). Whilst recognising its time and labour saving potential, they did not pursue it. Both The Met and South Wales are still using AFR, but before addressing them directly – and the even more controversial deployment of it by secretive and unaccountable "privately-owned public spaces" (Standing 2019:221-2) - we should note the context, in British, in which concern about police use of facial databases originated.

**The Origin of Political Concern**

Political concern about AFR technology In England and Wales segued from an initial concern about the photographic images ("mugshots") stored on the Police National Database (PNB). In 2012 the PNB contained an estimated 13 million "custody images" of faces, scars and tattoos (later revised to 21million - House of Commons Science and Technology Committee, 2019) taken in police stations at the point of arrest or charge. Although governed by a non-statutory code of practice – but unlike the existing DNA, fingerprint databases - there was no automated capability for removing images if suspects were not subsequently convicted. Such retention was ruled unlawful in the case R (RMC and FJ) v Metropolitan Police Commissioner, heard before the High Court in 2012. The Home Office was pressed with some urgency by the court to give the same protections to photographed citizens and suspects as were available on DNA and fingerprint databases. It promised action but it was 2015 before the Custody Image Review was initiated, and almost two more years before it reported, creating, not a legal requirement for removal on request, but only a presumption for it, if the police accepted that the person concerned was no longer a risk (Home Office 2017a). Because of this discretionary element, removal was not automated; it continued to be done manually.

The then Biometrics Commissioner, in particular, was uncomfortable with this limited response, and raised the concern with the enquiry into biometrics then being

undertaken by the House of Commons Science and Technology Committee (a cross-party group of Members of Parliament who can call on evidence and expert advice). The enquiry confirmed that three police forces were already using AFR, something which the Committee instinctively felt should have had a prior parliamentary mandate (as both DNA and fingerprinting did). The Home Office (2017b) flatly disagreed: "A decision to deploy facial recognition systems is an operational one for the police", wrote Baroness Susan Williams, the Minister of State for Countering Extremism (2017a). For good measure, if irrelevantly, she added that the High Court, in 2012, "did not rule that there was an issue with applying facial recognition software to images that were legitimately retained", which simply begged the question of where authority for mandating AFR *ought* to lie. In its May 2018 report, The House of Commons Committee emphasised its concern about the premature use of AFR, especially as concerns about its potentially discriminatory character had not been resolved. They indicated that the existing police trials should not be extended beyond their designated endpoint and that ministers and parliament, not the police themselves, should determine future police uses of AFR. They were unhappy that the Home Office had made or encouraged decisions in the absence of the forward-looking Biometrics Strategy promised in 2012, and that when the Strategy did appear in June 2018 it merely rationalised what the Home Office was already doing. More useful was an interim report from a working party commissioned by the Biometrics and Forensics Ethics Group (2019), published in February 2019, which teased out the ethical issues arising from the AFR deployments in The Met and South Wales, conceding their ambiguity of purpose, and outlined good practice in two useful appendices.

**The Metropolitan Police AFR Scheme**

The London police service used live AFR intermittently on ten occasions between 2016 and 2019, treating each deployment as a combined technology trial *and* a live operation which could lead to arrests. Most used unmarked mobile vehicles, some used cameras fastened on poles: posters and hand-distributed leaflets in the areas affected signalled that surveillance was occurring. The first deployments were a year apart, at the Notting Hill Carnival (a renowned, longstanding celebration if Afro-Caribbean culture in West London) in August 2016 and 2017. The third, (using a more accurate NEC algorithm, called M20) was on the Remembrance Sunday celebrations in Whitehall, central London in November 2017, attended by large crowds, senior politicians and members of the royal family. The fourth was outside London, with the Met assisting Humberside police with an operation in the port of Hull docks in summer 2018. The next two were in Stratford in the east of London, at Westfields, a vast shopping centre in the same period. The seventh and eighth were in Soho, a crowded entertainment area in central London in December 2018. The last two, using better cameras, were in Romford town centre in January, just outside London, in February 2019. Officers had constructed watchlists of people wanted by either police and courts, with just a smattering of volunteers faces on some of them. An eleventh non-operational AFR test, using only volunteers, took place in April 2019.

Two University of Essex researchers were participant observers in the mobile vehicles and the central control room in the last six operational deployments (Fussey and Murray 2019). Although the early deployments attracted the attention of Liberty, Big Brother Watch, and mainstream media, The Met gave no general information to the public until July 2018 when, fearing adverse publicity, it created an informative website, acquired a Twitter profile, opened up to the independent researchers and engaged in a dialogue with their critics, both pressure groups and politicians. Whether this in any way changed the intentions of the Met in respect of AFR is uncertain. As a Liberty spokesperson said:

> the police and the Home Office …. have been very reluctant to engage with the question of how facial recognition links in with other technologies, other developments, other databases, so concerns about the new LEDS database [the upcoming Law Enforcement Data Service is intended to replace the PNC] and how it might associate with that, concerns about where the photographs are coming from in the first place, how this might be used with body-worn video, how it might be used with CCTV (quoted in Fussey and Murray 2019:64-65)

Fussey and Murray provide a comprehensive, subtle, site-specific breakdown of how the AFR technology performed across each of the last six deployments, but their aggregated, headline figure about the 42 matches it made overall was that only 8 were unequivocally accurate, a poor " success" rate of only 19%. Presented thus, and combined with criticism of the way The Met constructed "watchlists" (sometimes ignoring its own criteria of "wanted by the police" to include people who were suspect for other reasons) made it easy to indict the trial. Fussey and Murray further also questioned the fusion of a trial with operational deployment, when the technology itself was not proven. They further strengthened their case against it with claims a) that the trial had no clear legal basis in the existing legislation on biometrics, and that b) The Met had not consistently proven, as the Human Rights Act 1998 requires, that AFR technology was proportional and "necessary in a democratic society" *across all the deployments*, supporting Big Brother Watch and Liberty on this. The Met was given a right of reply to these awkward findings and criticisms, but did not exercise it.

**The South Wales Police AFR Scheme**

South Wales formally began trialling FR in June 2017, with four police vans fitted with "pan, tilt and zoom" cameras, and clearly marked with "Facial Recognition Fitted" on the side, plus 14 additional cameras and 12 dedicated laptops at their disposal (Davies, Innes and Dawson 2018). Its first deployment In December 2017 at a European Champion's League football final between Real Madrid and Juventus, played at the Millenium Stadium in Cardiff, was rationalised as a preventive measure targetting individuals known for, or suspected of, football-related offences, and possibly subject to banning orders. Overall South Wales deployed their vehicles and/or fixed cameras at three music events, one football match, one boxing match, four "Six Nations" rugby matches and two sites intended to reveal suspects on outstanding police and court warrants. A short, non-operational deployment occurred after these to refine understanding of how the cameras performed under different conditions.

The Champion's League attracted a multi-national crowd of 170,000. 2470 potential matches were identified, of which an alarming 92% (2297) proved to be false positives. The South Wales Police later attributed this to the many "poor images" supplied by agencies, including UEFA and Interpol, but defended their general track record with FR since its introduction in June, with over 2000 accurate matches and 450 arrests and

> Successful convictions [which] so far include six years in prison for robbery and four-and-a-half years imprisonment for burglary. The technology has also helped identify vulnerable people in times of crisis. (A South Wales police spokesperson, quoted in Press Association 2018

Evidence from other deployments were not encouraging, 46 false positives at an Anthony Joshua boxing match and 42 at an Australia-Wales rugby match in November. Six matches at a major music event in Cardiff in December proved accurate. Cardiff University's independent evaluation of the scheme noted more positive results than were reported in the media (Davies, Innes and Dawson 2018), notably ….. South Wales Chief Constable, Matt Jukes, nonetheless fell back on the fear factor, possibly with the Manchester Arena suicide bombing on May 2017 in mind, pointing out that large gatherings were "potential terrorist targets". "We need to use technology when we've got tens of thousands of people in those crowds to protect everybody, and we are getting some great results from that," [he said] "But we don't take the use of it lightly and we are being really serious about making sure it is accurate"(quoted in Press Association 2018).

In May 2019, a former Liberal Democrat councillor, Ed Bridges, supported by Liberty, took South Wales Police to the High Court over the use of Automated FT. He first noticed the cameras during a lunchbreak, believing they had filmed him shopping and attending a peaceful demonstration against the arms trade. During the three day hearing, Liberty argued that AFT violated data protection and equality laws, not least because it was being trialled without proper public consent. In September 2019 two High Court judges ruled that South Wales *did have sufficient legal basis for it*:

> We are satisfied both that the current legal regime is adequate to ensure appropriate and non-arbitrary use of AFR Locate, and that South Wales Police's use to date of AFR Locate has been consistent with the requirements of the Human Rights Act and the data protection legislation (quoted in Bowcott 2019).

South Wales Police had always been confident about the potential of AFR. Even before the High Court's decision they were making to pilot the use of a FR app on 50 police officers' smartphones, so that, using a roadside snapshot of a suspect, they could check or confirm their identity without taking them back to a police station, instantly exposing those who might have given false information. This was considered proportionate, and officers involved were to receive specialised training and extra supervision. Liberty considered it "shameful" that South Wales Police were pressing ahead with this in advance of the upcoming court ruling (Sample 2019). Although Liberty appealed the High Court's judgement, The Met took it as a green light to proceed with its own *fully operational* deployment of AFR in 2020.

Independent research from Cardiff University into the South Wales deployment was designed-in from the outset, but Davies, Innes and Dawson (2018) took a different theoretical position, used a different methodology (which eschewed legal analysis) and drew more sympathetic conclusions than Fussey and Murray had in The Met. South Wales trialled both the live "locate" and office-based "identify" functions of the AFR system provided by NEC, and the researchers evaluated both separately. They examined organisational performance (how the technology was implemented in the police force), system performance (technical capabilities and outcomes), and operator performance (the behaviour and decision making of officers interacting with the technology). Whilst giving more technical details about AFR, they placed an overriding emphasis on it as "a socio-technical system" whose effectiveness was never simply an artefact of algorithmic matching but a product of the way officers interacted with it, eg in terms of manually configurable settings as to image resolution, the compilation of watchlist size, and the requirement for human confirmation of any image's accuracy. Davies, Innes and Dawson (2018) thus

preferred to designate the police practice as "*assisted* facial recognition" or even "*automated assisted* facial recognition", in order to avoid the impression that the algorithm operated autonomously – a more flexible approach than that taken by Fussey and Murray in respect of The Met. Technical quality and reliability nonetheless matters because of its impact on officer confidence: the first algorithm (S17) provided by NEC performed poorly (eg at the Champion's League) in terms of matches and gender recognition, diminishing officer's personal investments in the approach. South Wales requested an improvement, and the second algorithm (M20) made a marked, decisive improvement, and led the researchers judge the trial a qualified success:

> Overall, the proportion of true positives increased from 3% at the initial Champions League deployment to 46% at the [final] Six Nations deployments. This was due to both the new algorithm and increased operator familiarity with the system settings (Davies, Innes and Dawson 2018:8)

South Wales Police, unlike the Met, had engaged the media from the outset in respect of the AFR scheme and engaged with the public via a Facebook page. Public comment on the latter was mixed with both praise for the new initiative and ominous comparisons with Orwell's *Nineteen Eighty Four*. Journalists tended to find failings more newsworthy than success more put a critical spin on events, even when they had access to balanced information, although Davies, Innes and Dawson didn't deny that ethics and accountability issues needed airing and that existing regulatory frameworks needed revision. When watching the live deployments they felt that the public generally reacted positively, and that approaches to persons of interest who turned out not to be the match were mostly resolved amicably. In their concluding discussion about ethics and legality they responded to claims about the inherently discriminatory character of AFR technology. They didn't dispute its possibility, but said of South Wales that

> although we have been unable to systematically test it, the indications from the evidence accumulated by this evaluation are that watchlist composition and configuration plays an important role in shaping AFR accuracy and precision in terms of generating 'true positive' and 'false positive' results. During the evaluation period, no overt racial discrimination effects were observed. But this could potentially be an artefact of the demographic make-up of the watchlists utilised (Davies, Innes and Dawson 2018:41).

Notwithstanding their differences of emphasis, the combined breadth and sophistication of the research reports into the two ongoing police deployments of AFR in England and Wales, yield insight and add considerably to transferable knowledge about it. Given the manifestly complex legal, ethical and practical issues that AFR raises within the police, it is all the more concerning that a possibly unknown number of privately-owned public spaces in England and Wales have also deployed it, with no equivalent transparency.

**Facial Recognition in Privately-Owned Public Spaces**

In August 2019 it was revealed by the *Financial Times* (Murgia 2019) that property developer Argent, as part of a consortium with Hermes Investment Management, on behalf of BT Pensioners, and AustralianSuper (another pension scheme) had been covertly using FR within CCTV systems in and around Granary Square, a 67-acre, 50-building site in London north of Kings Cross railway station. This is an upmarket commercial, residential and recreational area, used by thousands of people daily, encompassing Google's London HQ, the Central St Martin's Art School and, on its fringes, *The Guardian's* own HQ. The cameras

fitted with FR were not easy to identify – no special signage was used. When pressed, Argent could say no more about the purposes of their FR than that it was "in the interests of public safety and" – even more ominously - "to ensure that everyone has the best possible experience". Argent conceded that it used "number of detection and tracking methods, including facial recognition" within the area, without indicating whether anyone was specifically targeted, or the nature of the privacy safeguards they said were in place (quoted in Sabbagh 2019a). Camden, the local government area in which Granary Square was set, was unaware of it. A small random survey of people living and working in the area affected registered both unease and ambivalence about the revelation, some people not minding the presence of FR simply because of already ubiquitous data extraction, but most were alarmed by the scheme's secretiveness and lack of transparency (see Busby 2019).

This was also what concerned both the civil liberty groups and official regulators about the King's Cross development. Liberty's denunciation of it as "a disturbing expansion of mass surveillance that threatens our privacy and freedom of expression as we go about our everyday lives" (idem) was unsurprising, but Tony Porter, the Surveillance Camera Commissioner used it to highlight the absence of legislation to regulate FR developments. Within days, Elizabeth Denham, the Information Commissioner, which was investigating the use of FR in the private sector, asked Argent to clarify the legal basis of its technology. She was reported as saying:

> Scanning people's faces as they lawfully go about their daily lives in order to identify them is a potential threat to privacy that should concern us all. That is especially the case if it is done without people's knowledge or understanding (quoted in Rawlinson 2019).

Sadiq Khan, the Mayor of London did the same, picking up on its potentially discriminatory consequences, insisting that public spaces "should be places that all Londoners, regardless of their age, ability, gender, gender identity, religion, race, sexual orientation or social class, can enjoy and use confidently and independently, avoiding separation or segregation" (quoted in Sabbagh 2019b). Somewhat embarrassingly for Khan, on the very same day as the High Court judgement in relation to South Wales Police, he admitted that the Metropolitan Police were in fact sharing facial images with Argent's Granary Square project between 2016 and 2018.

Granary Square proved not to be unique. Big Brother Watch went on to reveal that a number of commercially-owned shopping centres, museums, conference centres and music venues were using, or had used facial recognition technology. Among them Sheffield's Meadowhall (in 2018, in a trial supported by the police) and currently Birmingham's Millennial Point conference centre (also in conjunction with police). Manchester's Trafford Centre had been checking every visitor – an estimated 15 million - against a database of 30 faces before it was stopped by the ICO in 2018, on the grounds that its deployment affected so many ordinary people (Sabbagh 2019). A linked group of museums in Liverpool have piloted it, and indicated they may use it again. Madhumita Muria (2019) also revealed last August that Canary Wharf Group, manager of a 97-acre premier business and residential district in London which already operates 1750 CCTV cameras and an automated number place recognition (ANPR) scheme, was negotiating with tech suppliers "to install facial recognition". She also discovered that supermarkets Tesco, Sainsbury's, Marks and Spencer, as well as convenience stores Budgen's, all anticipated using FR, for "crime prevention and estimating the age of those buying cigarettes or alcohol" (Muria 2019). The exact number of

private sector deployments of facial recognition in Britain, which flourish in the absence of prohibition, are not known.

**Developments in 2020**

The Metropolitan Police announced in January 2020 that it would selectively deploy live facial recognition (LFR) technology later that month. The database would be limited, containing only the faces of suspects associated with serious and violent behaviour, based on recent intelligence in particular areas. The programme would be overt, pursued for a only a few hours at a time, and done in consultation (handing out leaflets) with the specific communities affected. All alerts, say the Met, will be quickly checked for accuracy before action is taken: anyone who turns out not to match a face on the database will have their image deleted immediately, otherwise they will be spoken to by an officer, and presumably arrested. Although the Met are now claiming a 70% match rate – Pete Fussey's research had stated 19% - they concede that the current technology is not ideal for scanning dense crowds (and maybe less good in artificial light at night than in daylight) they are claiming strong public support for the initiative. The localised nature of the databases being used is a concession to Sadiq Khan, the Mayor of London, based on an independent ethics review: they will not be linked to other databases and will not enable tracking-by facial-recognition across London as a whole.

In South Wales, the favourable High Court ruling has settled nothing, especially among football fans. At the championship game between Cardiff City and Swansea on Sunday 12 January 2020 a pre-match protest was organised jointly by Big Brother Watch and Cardiff City Supporters Club, who unfurled a banner outside the ground saying "No Facial Recognition". Marked vans were seen patrolling roads around the stadium, with one stopping outside a pub regularly frequented by Cardiff fans. The protest was cheerful but some fans wrapped scarves round their faces, and wore glasses, hoods, and/or masks. *The Guardian* reported a selection of fans comments as follows:

> "It feels as if every single person is under scrutiny now. I haven't seen trouble here for 10 years."
>
> "It's intimidating. The authorities that are there to protect us are attacking our rights.
>
> "Football has made massive steps. The police do a wonderful job, but this is one step beyond. We're becoming the most watched city in Europe. I think we need more boots on the ground rather than cameras."
>
> "I think the use of this technology is disproportionate to the risk this game poses. It infringes on people's right to privacy. I think there's an ulterior motive – South Wales police are trialling it and they think they can get away with using it at football matches. (quoted in Morris 2020)

More surprisingly, in advance of the game, Arfon Jones, a former long-serving police officer, by then the North Wales Police and Crime Commissioner (an elected office, to hold local police forces accountable), had implicitly criticised his South Wales counterpart (and the High Court) for supporting the AFR deployment. Jones described its use in Cardiff as "disproportionate", questioned its accuracy, warned against its discriminatory potential and recalled, for good measure, the fiasco of false positives at the Millenium Stadium in December 2017. He characterised it as a "fishing expedition where, once again, football

fans are being unfairly targeted in a way that *supporters of other sports are not*" (which was not strictly true). He went on:

> It's a step too far and creates the potential for miscarriages of justice. I'm sure there are people from North Wales who will be going down to the game and risk having pictures taken of them without their consent. I have a responsibility to represent them and to oppose fishing expeditions that invade their privacy. ." (Quoted in MacDonald 2020

What are the prospects for AFR on the national scene, given Britain's unfolding separation from the European Union (EU) (aka Brexit)? The EU's groundbreaking General Data Protection Regulation (GDPR) legislation of May 2018 briefly heightened national debate on data-privacy. It have constrained some, but obviously not all, police forces (who could claim some exemptions from it) from pursuing AFR, and perhaps even some privately-owned public spaces thought twice about it. Government itself was unconstrained, and with already Brexit "in the air" at this time, deference to European legislation may not have seemed unduly pressing. As Brexit proceeds, the prospect of repealing the 1998 Human Rights Act looms closer, although many groups will contest this. Long reviled by the now dominant right-wing of the Conservative Party, they would replace it with a legally fiercer, home-grown, Bill of Rights, obviating requirements for national criminal justice practices to accord with internationally recognised human rights standards.

But Europe itself is somewhat ambivalent about facial recognition technologies, GDPR\s requirement that EU citizens should not be the "subject of a decision-based solely on automated processing, including profiling". The EU has in fact funded controversial border control trials in Hungary, Latvia and Greece using "deception detection" technology dubiously based on reading facial micro-expressions (Boffey 2018). The European Parliament actually considered using AI-assisted translation services and facial recognition for internal security as part of their own "digital transformation programme", but after an outcry by some MEPs and staff unions the latter was abandoned (Rankin 2020). The European Commission's (2020) White Paper on the regulation of AI fell short of banning AFR specifically, but was concerned about the speed at which it was spreading in Europe, not only in the three English police forces, but also in German plans for their use in airports and train stations (following a pilot in Berlin), French plans to use facial biometrics as a means of access control for citizens using secure government websites, and eastern European border management (Boffey 2020). The Commission focussed on regulating applications of AI more generally, rightly seeing AFR as an aspect of this.

Back in Britain, Scotland, always more mindful of EU concerns, and with its own history of concern about the police storage of "custody images", is distancing itself from practice in England and Wales, and seeking to pre-empt the use of live AFR in Police Scotland (a nationwide police force), which had indicated in a 10-year plan its intention to use it before 2026. In February 2020, the Justice Sub-Committee for Policing of the (devolved) Scottish Parliament stated that there could be no justification for it, because it was "known to discriminate against females, and those from black, Asian and ethnic minority communities", was at odds with the Scottish tradition of policing by consent and ostensibly at variance with the requirements of human rights and data protection legislation. The Sub-Committee stopped short of demanding a complete ban and, in democratic deference to competing views and interests on technology's role in public safety, concluded that

> this short inquiry has highlighted the pressing need for a much wider debate on the use of live facial recognition technology by the police service, as well as more widely across the public sector, and by private companies. Politicians could play a key role in determining whether there is public consent for the use of this technology (Scottish Parliament 2020).

In fact, something is known about UK-wide public attitudes towards AFR. In summer 2019 the Ada Lovelace Institute (2019) (a British think tank "with a mission to ensure data and AI work for people and society") commissioned a survey of 4109 nationally representative adults to ascertain their views on emerging AFR technologies in law enforcement, retail, education. There are six key findings. The first is that while AFR is known about, there is no deep understanding of it, warranting "more informed public debate". Secondly consent to its use matters and there should be a right to opt out of it. Thirdly a majority support AFR which has a "demonstrable public benefit" but expect this to be focussed and limited: they do not want it banned, but nor do they want it normalised. Fourthly, police use is only legitimate if there are clear safeguards – there is no "unconditional support" for it. Fifthly, the private sector is not trusted to use AFR ethically. Sixthly, vendors should cease supplying police with AFR until it has been better tested and governments should place limits on its use, even in the police.

**Conclusion**

There is cause for concern about the way AFR is developing in England and Wales, although it may not be unique in that respect. The Conservatives government's failure to propose and implement regulatory legislation occurred despite a deeply informed understanding of the promise and perils of emerging AFR technology, none more so than among the state's own data commissioners. They have made all the requisite warnings, but despite their concerns, supported by several civil libertarian groups, liberal media, independent researchers, and a parliamentary committee, the piecemeal expansion of AFR in England and Wales is set to continue. Why is this so?

The Conservative government's failure to enact regulatory legislation might charitably be attributed to the squeezing of parliamentary time during the intensifying debates on Brexit between 2016-2019. It is arguable, however, that government never really wanted to regulate, and were, for ideological reasons, quite content to let police and market-led AFR initiatives occur unimpeded. From 2010 onwards, government had itself encouraged disruptive technological innovation in public services, looking to the private sector to stimulate solutions, and pursuing a "digital by default" agenda which would achieve the fabled "more for less" in service delivery during the years of austerity (Babuta and Oswald 2020). "Big" government regulation, they reasoned, would have slowed or stifled innovation. Thus, by "failing" to devise a Biometric Strategy the Home Office deliberately left both police forces and private operators with a freer hand than they may otherwise have had, and, in effect, endorsed their initiatives.

Given the likelihood of AFR developing further in England and Wales, a lot will ride on such non-statutory regulation as has come into being, namely the *advisory* ethical statement in Appendices A and B of the Biometrics and Forensics Ethics Group (2019), followed a month later by the publication of the Surveillance Camera Commissioner's (2019) own detailed *voluntary* code of practice. Will public agencies and private organisations abide by them? Neither document is enforceable, but, like the two research reports, they are intellectually exemplary documents, cogent, pragmatic and respectful of democratic

concerns, except the big one: the vital question of whether England and Wales should have adopted AFR in the first place – a decision that, ideally, government itself should make - and whether we should leave agencies and organisations the freedom to determine its future.

Given the current balance of forces in the argument, the prospect of a localised, US-style ban on AFR by any urban municipality in England and Wales, let alone a fully national one, will not happen. Even a moratorium on operational trials until such time as AFR has been perfected is unlikely, because The Met have already decided that operationally "good enough" equipment is already available on the market. Unsurprisingly, the National Police Chief's Council (website) insists that "the use of new techniques and technologies such as body worn video, facial recognition or artificial intelligence for public good is essential for the future of policing in the modern world", alongside the familiar reassurances about transparency, accountability and privacy. While there are senior police managers who share the Surveillance Camera Commissioner's and the Ada Lovelace Institute's concern that indiscriminate use of AFR could indeed undermine police legitimacy, and would prefer statutory regulation to voluntary compliance with codes of practice, the broad direction of travel with this technology is already clear.

Talking up the case for a ban on AFR at least has the merit of problematising it, casting doubt on its alleged indispensability to fighting crime and refusing to normalise it. Surprisingly to some, Bruce Schneier (2020), an often critical US commentator on overblown "security theatre", is himself sceptical of attempts to single out and ban AFR, believing that this misses the bigger picture of what is at stake. Unlike earlier police use of biometrics and CCTV, AFR is simply one of many expressions of the way in which AI is being used to influence consumer behaviour, inform policing, and regulate eligibility for welfare services – "automating inequality", as Virginia Eubanks (2015) puts it – and it this bigger picture which should be brought into focus, analysed and resisted. The latest contribution to this debate in Britain, from the Royal United Services Institute (RUSI – a respected "defence and security" think tank) makes the same point, and indeed the European Commission's point about AI – it is the whole move towards "data-driven policing", of which AFR is just one aspect, that needs proper regulation (Babuta and Oswald 2020). The government in England and Wales has thus far not been receptive to this. Scotland might be. How this is plays out internally in a volatile, post-Brexit Britain, and whether there will be any alignment with the views of the European Commission on AI, remains to be seen.

**References**

Ada Lovelace Institute (2019) *Beyond Face Value; public attitudes towards facial recognition.* London: Ada Lovelace Institute

Babuta A and Oswald M (2020) *Data Analytics and Algorithmic Bias in Policing*. London: Royal United Services Institute.

BBC News (2020) Russia's use of facial recognition challenged in court. 31 January 2020

Big Brother Watch (2018) *Face Off: the lawless growth of facial recognition in UK policing.* London: Big Brother Watch

Biometrics and Forensics Ethics Group (2019) *Interim Report of the Facial Recognition Working Party.* Home Office: Biometrics and Forensics Ethics Group

Boffey D (2018) EU border 'lie detector' system criticised as pseudoscience. *The Guardian* 2.11.18

Boffey D (2020) EU eyes temporary ban on facial recognition in public places. *The Guardian* 17.1.2020

Bowcott O (2019) Police use of facial recognition is legal, Cardiff high court rules. *The Guardian* 4.9.2o19

Busby M (2019) People at King's Cross site express unease about facial recognition. *The Guardian* 13.8.2009.

Buolamwini J and Gebru T (2018): Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification. In *Proceedings of Machine Learning Research* 91:1, p.1-15. Available from http://proceedings. mlr.press/v81/buolamwini18a/ buolamwini18a.pdf, p.1.

Davies B, Innes M and Dawson (2018) *An evaluation of South Wales Police's use of Automated Facial Recognition*. Cardiff: Cardiff University Police Science institute.

Dodd V (2020) Met police to begin using live facial recognition cameras in London. *The Guardian* 24.1.20

Eubanks V (2015) *Automating Inequality: how high-tech tools profile, police and punish the poor*. New York: St.Martin's Press

European Commission (2020) *White Paper: On Artificial Intelligence - A European approach to excellence and trust.* Brussels: European Commission

Feldstein S (2019) *The Global Expansion of AI Surveillance*. Washington: Carnegie Endowment for International Peace.

Fussey P and Murray D (2019) *Independent Report on the London Metropolitan Police's of Live Facial Recognition Technology*. University of Essex: Human Rights centre

Hare S (2019) Facial recognition is now rampant. The implications for our freedom are chilling. *The Guardian* 18.8. 2019

Hill K (2020) The Secretive Company That Might End Privacy As We Know It The New York Times 8.1.2020

Home Office (2017) Letter from the Minister of State for Countering Extremism to the Chair of the House of Commons Science and Technology Committee: *Publication of The Home Office Biometrics Strategy and Government Policy on Police Use of Facial recognition* Systems. 30th November 2017 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/171130-BWT-to-Chair-biometric-strategy.pdf

Home Office (2017b) *Review of the Use and Retention of Custody Images.* London: Home

Office

House of Commons Science and Technology Committee (2019) *The work of the biometrics commissioner and the forensic science regulator inquiry*. London: House of Commons

Kaltheuner F (2020) Face scanning cameras will put us all into an Identity parade. *The Guardian* 27.1.2020

MacDonald H (2020) Facial recognition at South Wales derby 'a step too far', says police chief. *The Guardian.* 8.1.2020

Morris S (2020) Anger over use of facial recognition at south Wales football derby *The Guardian.* 12.1.2020

Muria M (2019) London's King's Cross uses facial recognition in security cameras. *Financial Times.* 12 8.2019

Press Association (2018) Welsh police wrongly identify thousands as potential criminals. *The Guardian.* 2.5.218

Rankin J (2020) European Parliament will not use Facial recognition technology. *The Guardian.* 5. 2. 2020)

Rawlinson K (2019) ICO opens investigation into use of facial recognition in King's Cross. *The Guardian.* 15.8.20

Sabbagh D (2019a) Regulator looking at use of facial recognition at King's Cross site *The Guardian* 12. 8. 19

Sabbagh D (2019b) London mayor writes to King's Cross owner over facial recognition. *The Guardian.* 13.8.2019

Sample I (2019) South Wales police to use facial recognition apps on phones. *The Guardian.* 7.8.19

Scottish Parliament (2020) *Facial recognition: How Policing in Scotland makes use of this technology.* Report from the Justice Sub-Committee on Policing. Edinburgh: Scottish Parliament.

Standing G (2019) *Plunder of the Commons: a manifesto for sharing public wealth*. London; Penguin Book

**Words 7522**