Article:
Purshouse, J. and Campbell, L. (2022) Automated facial recognition and policing: a Bridge too far? Legal Studies, 42 (2). pp. 209-227. ISSN: 0261-3875

https://doi.org/10.1017/lst.2021.22

Automated facial recognition and policing: A Bridge too far?

Joe Purshouse[1*] and Liz Campbell[2†]

[1]University of East Anglia and [2]Monash University

*corresponding author e-mail: J.Purshouse@uea.ac.uk

Keywords: *Criminal Justice; Policing; Automated facial recognition technology*

Automated facial recognition (AFR) is perhaps the most controversial policing tool of the twenty-first century. Police forces in England and Wales, and beyond, are using facial recognition in various contexts, from evidence gathering to the identification and monitoring of criminal suspects. Despite uncertainty regarding its accuracy, and widespread concerns about its impact on human rights and broader social consequences, the rise of police facial recognition continues unabated by law. Both the Government and the domestic courts were satisfied that police use of this technology is regulated adequately by existing statutory provisions regulating the processing of data and police surveillance generally. That is, until the recent judgment of the Court of Appeal in R. (Bridges) v Chief Constable of South Wales Police and ors *[2020] EWCA Civ 1058, where it was held that the respondent's use of AFR was unlawful. This article provides an analysis of AFR, reflecting on the outcome of that case and evaluates its nuanced findings. We suggest that the judgment leaves considerable room for police AFR to continue with only minor, piecemeal amendment to the legal framework. Drawing on comparative experience and relevant socio-legal scholarship, we argue that the relatively unfettered rise of police facial recognition in England and Wales illuminates deeper flaws in the domestic framework for fundamental human rights protection and adjudication, which create the conditions for authoritarian policing and surveillance to expand.*

1. INTRODUCTION

Rapid advances in technology are disrupting the balance of power between governors and the governed. Automated facial recognition technology (henceforth, AFR) is not the only biometric surveillance technology that is in ascendency and posing challenges for law, but it is perhaps the one that has most captured the public imagination. AFR is an algorithmic technology. AFR algorithms are developed to locate a face within an image, measure the geometric features of the face (distance between eyes, width of mouth etc), and then 'match' the face to a previously stored image of the individual (usually stored on a watchlist or database), based on the strength of the correlation between geometric features.[1] It has numerous applications, such as

† Thanks to Austin Bond for research assistance. The authors are also grateful to the anonymous reviewers for their insightful suggestions and comments.

[1] J Fong, 'What facial recognition steals from us' (*Vox*, 10 December 2019), available at: https://www.vox.com/recode/2019/12/10/21003466/facial-recognition-anonymity-explained-video

automating border identity verification checks,[2] pupil registration in schools,[3] or enabling more effective photo sharing on social networking sites.

AFR is being utilised by law enforcement agencies across the world to fulfil various functions. In some jurisdictions with autocratic political regimes, AFR has been used for overt repression and persecution. One egregious example is the Communist Party of China, which has invested heavily in developing the infrastructure to pervasively monitor and control citizens. In 2015, Party officials called for an acceleration of public security video monitoring systems in order to achieve 'systematic and dense coverage' of all public areas.[4] In particular, the Party has targeted its Uyghur Muslim population in the Xinjiang region, installing AFR cameras, supplied by global surveillance manufacturer Hikvision, at the entrances to 967 mosques.[5] Most security checkpoints stationed along Xinjiang's major roads now employ facial recognition cameras of varying sophistication.[6] The technology is facilitating the Communist Party of China's authoritarian control of the region, where internment in 're-education camps' and other human rights abuses of the Uyghur population have been well documented.[7]

Chinese AFR surveillance infrastructure is also being purchased and utilised by Governments in developing nations, such as Uganda and Zimbabwe.[8] Other autocratic regimes are looking to AFR to strengthen controls on their citizens' movements. In January 2020, Amnesty International reported that Russian authorities plan to operationalise a large-scale facial recognition system covering the whole Moscow Metro transportation network.[9] Whilst the use of AFR in these jurisdictions is not constrained by the checks and balances of jurisdictions with stronger legal human rights protections, the fast-paced expansion of experimental AFR in jurisdictions with broad commitments to liberal democracy, without prior parliamentary approval, raises legitimate questions concerning the effectiveness of the operation of any such checks and balances. Particularly, as to whether these checks and balances are robust enough to harness law enforcement to operate within the constraints of human rights law *before* experimental forms of surveillance technology are deployed.

---

[2] Such as in the European Union's proposed automated Entry/Exit System. See Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017.
[3] M Andrejevic and N Selwyn, 'Facial recognition technology in schools: critical questions and concerns' (2020) 45 Learning, Media and Technology 115.
[4] Z Zhengfu 'Zhonggong zhongyang bangongting, guoquyuan bangongting yinfa "guanyu jiaqiang shehui zhi'an fangkong tixi jianshe de yijian"' [The CCP CC General Office and State Council General Office issue 'Opinion on building a system to strengthening public order and control'] (*Xinhua*, April 13 2015), available at: http://www.gov.cn/xinwen/2015-04/13/content_2846013.htm. Quoted in J Leibold 'Surveillance in China's Xinjiang region: ethnic sorting, coercion, and inducement' (2019) 29 Journal of Contemporary China 46.
[5] E Feng 'China steps up surveillance on Xinjiang Muslims' (*Financial Times*, 18 July 2018), available at: https://www.ft.com/content/c610c88a-8a57-11e8-bf9e-8771d5404543.
[6] Ibid.
[7] P Mozur 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority', (*New York Times,* 14 April 2019), available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[8] A Gross et al 'Chinese tech groups shaping UN facial recognition standards' (*Financial Times,* 2 December 2019), available at: https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.
[9]Amnesty International UK 'Russia: Legal challenge to 'intrusive' facial recognition technology' (Media Release, 31 January 2020), available at: https://www.amnesty.org.uk/press-releases/russia-legal-challenge-intrusive-facial-recognition-technology?gclid=EAIaIQobChMItomcqKC46AIVWeDtCh0YegIcEAAYASAAEgKz-PD_BwE.

In the United States,[10] Australia,[11] and several EU Member States,[12] AFR has been used by police forces to monitor public spaces, and to retrospectively identify suspects by running CCTV images collected from a crime scene against police databases. Furthermore, the COVID-19 pandemic has prompted the use of facial recognition software to ascertain if someone is wearing a mask, the amendment of algorithms to be able to identify someone who is wearing a mask, and also AFR's combination with thermal imaging to determine if someone has a temperature, which is a common symptom of COVID-19. Such uses are evident in public spaces, workplaces and vulnerable/hotspot locations like aged-care facilities.[13]

In England and Wales, police forces have used the technology for retrospective identification,[14] and to identify suspects in their custody.[15] AFR has also been used by police at a number of public gatherings to identify 'persons of interest' in real time. Owing to concerns over its impact on human rights, the police use of AFR has sparked public protests[16] and counter-surveillance reactions, including the use of face coverings,[17] and the tactical use of lasers to obstruct AFR apparatus.[18] Civil liberties group, Liberty, has campaigned to ban the police use of AFR altogether, particularly in public spaces.[19] So far, these calls have been resisted by English lawmakers but, as we shall discuss, the regulation of police AFR has been, and continues to be, an evolutionary process. In September 2019, the High Court of Justice in *R (Bridges) v The Chief Constable of South Wales,* held that the law permits police the discretion to use AFR for various operational functions.[20] The Divisional Court found in the respondent's

[10] S Ghaffary 'How to avoid a dystopian future of facial recognition in law enforcement' (*Vox*, 10 December 2019), available at: https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation.
[11] A Bogle 'Australian Federal Police officers trialled controversial facial recognition tool Clearview AI' (*ABC News*, 14 April 2020), available at: https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894.
[12] European Union Agency for Fundamental Rights *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (27 November 2019); L Kayali, 'How facial recognition is taking over a French city' (*Politico,* 26 September 2019), available at: https://www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city/.
[13] C Burt 'Facial recognition temperature scanning, wearables and voice biometrics deployed for COVID-19 spread prevention' (*Biometric Update,* 3 August 2020), available at: https://www.biometricupdate.com/202008/facial-recognition-temperature-scanning-wearables-and-voice-biometrics-deployed-for-covid-19-spread-prevention.
[14] Centre for Data Ethics and Innovation *Snapshot Paper-Facial Recognition Technology* (28 May 2020) para [5.2], available at: https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology.
[15] Universities' Police Science Institute and Crime & Security Research Institute *An Evaluation of South Wales Police's Use of Automated Facial Recognition* (Cardiff, 2018) p 30, available at: https://afr.south-wales.police.uk/wp-content/uploads/2019/10/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf.
[16] 'Fans stage protest against use of facial recognition technology ahead of Cardiff v Swansea match' (*ITV News*, 12 January 2020), available at: https://www.itv.com/news/wales/2020-01-12/fans-stage-protest-against-use-of-facial-recognition-technology-ahead-of-cardiff-v-swansea-match/.
[17] A Hearn 'Anti-surveillance clothing aims to hide wearers from facial recognition' (*The Guardian,* 4 January 2017), available at: https://www.theguardian.com/technology/2017/jan/04/anti-surveillance-clothing-facial-recognition-hyperface.
[18] A Cuthbertson 'Hong Kong protesters use lasers to avoid facial recognition cameras and blind police' (*The Independent*, 1 August 2019), available at: https://www.independent.co.uk/news/world/asia/hong-kong-protests-lasers-facial-recognition-ai-china-police-a9033046.html.
[19] I Sample 'Facial recognition tech is arsenic in the water of democracy, says Liberty' (*The Guardian*, 8 June 2019), available at: https://www.theguardian.com/technology/2019/jun/07/facial-recognition-technology-liberty-says-england-wales-police-use-should-be-banned.
[20] *R (Bridges) v The Chief Constable of South Wales* [2019] EWHC 2341 (Admin).

favour despite 'the lack of a clear legislative framework for the technology'.[21] Indeed, the Protection of Freedoms Act 2012 provides a legal framework for two types of biometrics, DNA and fingerprints, but does not apply to other biometrics such as facial images, gait, or voice. In August 2020, the Court of Appeal allowed the claimant's appeal on the grounds that the South Wales Police's (SWP) use of AFR was unlawful as it was not 'in accordance with law' for the purposes of Article 8(2) of the European Convention on Human Rights (ECHR), and the SWP had failed to carry out a proper Data Protection Impact Assessment (DPIA). The SWP also failed to comply with the public sector equality duty (PSED). This was reportedly the first successful legal challenge to AFR technology use in the world.

This article subjects the decisions in *Bridges* and, more broadly, the Government's position on the legality of police AFR use, to critical scrutiny. It will argue that the legal basis for police AFR surveillance is inadequate, and that the legal framework regulating the police use of this technology is too imprecise to protect citizens from abuse or arbitrariness. Drawing on the experience of other common law jurisdictions, and relevant socio-legal scholarship, the article suggests that this framework and its interpretation in domestic courts transforms human rights protection into a tick-box exercise, foreclosing important political debate on the normative consequences of police AFR surveillance. English and Welsh police forces have been afforded too much discretion to 'widen the net' of biometric surveillance, without explicit democratic approval.

2. AFR IN ENGLAND AND WALES

Since at least 2014, several police forces in England and Wales have trialled the use of AFR in several contexts. AFR is used in three broad ways:

1. Identity verification
A suspect is arrested but refuses to provide their name to police. Here, police could take a static 'probe image' of the individual's face. AFR software could then be used to verify the individual's identity by comparing the probe image against a database of images that the police control, or to which the police have access.

2. Retrospective or speculative identification
CCTV footage shows a suspected burglar leaving a property. A still of the suspect's face is used as a probe image and compared with a database of custody images (commonly known as 'mugshots'). The AFR software generates a shortlist list of possible matches, and police arrest a suspect based on their place of residence being close to the crime scene and the strength of the AFR 'match'.

3. Live AFR
A live deployment of AFR may be used to identify 'persons of interest' to the authorities as they traverse a vicinity of public space. Live AFR typically involves the deployment of surveillance cameras to capture digital images of members of the public, which are then compared with digital images of persons on a pre-assembled 'watchlist' of images the police have compiled for the purpose of the deployment.

[21] House of Commons Science and Technology Committee *The Work of the Biometrics Commissioner and the Forensic Science Regulator,* Nineteenth Report of Session 2017–19, HC 1970, 18 July 2019 (HMSO, 2019) at p 29.

The decision to use or not use AFR in a particular context is value-laden. Tensions between competing values and aims arise at different points in the development, deployment and maintenance of AFR, as with any other algorithmic system.[22] For example, the use of AFR for identity verification will be more accurate and safe than for a live AFR system, as it will involve the comparison of one clear and static image with another, also likely of high quality (a one: one comparison). Live AFR is likely to involve a 'one to many' comparison, that is, a target image with a database of subjects, or 'many to many' search, dataset to dataset. The live system may also bring into play human rights considerations that do not apply when utilising the first type (eg it may have a disruptive 'chilling' effect on public assemblies if used to monitor crowds at a protest or sporting event[23]). Likewise, speculative identification through AFR may raise issues pertaining to criminal procedure and fair trial rights that do not arise with other types of AFR, when these are used in a non-investigative capacity.[24]

In England and Wales, several police forces have experimented with the use of AFR in numerous contexts. The most prominent trials have been conducted by Leicestershire Police, SWP, and the Metropolitan Police Service (MPS).[25] The MPS has since gone beyond trialling the technology, adding AFR to their operational public surveillance arsenal.[26]

Domestic forces have also collaborated with private organisations to engage in AFR surveillance activities. In August 2019, it was reported that several commercial landowners were using AFR surveillance on their publicly accessible land.[27] In September of the same year, the Metropolitan Police acknowledged that it had supplied images of individuals for one commercial landowner to use when deploying AFR at its site in the Kings Cross area of London.[28] In January 2020, the New York Times reported that a small AFR start-up company, Clearview AI, had sold its AFR tool to over 600 law enforcement agencies around the world, and a number of police forces based in the UK had accessed the Clearview AI database. The tool, which 'scrapes' and compares photos without consent from online platforms, is described as follows:

---

[22] N Lynch, L Campbell, J Purshouse and M Betkier *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (November 2020); The Law Society Commission on the Use of Algorithms in the Justice System and The Law Society of England and Wales *Algorithms in the Criminal Justice System* (June 2019) p 4.

[23] J Purshouse and L Campbell 'Privacy, crime control and police use of automated facial recognition technology' [2019] Criminal Law Review 188.

[24] C Garvie *The Perpetual Line-Up: Unregulated Police Face Recognition in America in 2016*.

[25] For further detail see above n 23.

[26] A Satariano, 'London police are taking surveillance to a whole new level' (*New York Times*, 24 January 2020), available at: https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html?auth=login-email&login=email.

[27] In London, the use of AFR surveillance by property developer, Argent, on its publicly accessible land in the Kings Cross area of the city prompted public disquiet and an investigation by the Information Commissioner's Office. See M Murgia 'London's King's Cross uses facial recognition in security cameras' (*Financial Times*, 12 August 2019), available at: https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c. See also: AR Cuthbert and KG McKinnell 'Ambiguous space, ambiguous rights – corporate power and social control in Hong Kong' (1997) 14 Cities 295; D Sabbagh 'Regulator looking at use of facial recognition at King's Cross site' (*The Guardian,* 12 August 2019), available at: https://www.theguardian.com/uk-news/2019/aug/12/regulator-looking-at-use-of-facial-recognition-at-kings-cross-site?CMP=share_btn_link.

[28] L Kelion 'Met police gave images for King's Cross facial recognition scans' (*BBC,* 6 September 2019), available at: https://www.bbc.co.uk/news/technology-49586582.

> You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system — whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites — goes far beyond anything ever constructed by the United States government or Silicon Valley giants.[29]

Many of Clearview AI's clients, including several UK and Australian police forces, had not previously disclosed or indeed had denied their use of the app to the public, and had no internal guidance or policies regulating the circumstances in which they might use the app.[30] The Information Commissioner's Office and its Australian counterpart have opened a joint investigation into Clearview AI's personal information handling practices.[31]

The rise of AFR has not been frictionless. Civil liberties organisations, such as Liberty, various academics (including the authors of this paper) as well as the Home Office Biometrics and Forensics Ethics Group, have raised concerns that the police use of AFR lacks a firm legal basis, and poses an acute threat to various human rights, including the rights to privacy, free association, and freedom from discrimination.[32] In July 2019, the House of Commons Science and Technology Select Committee called on the Government to issue a moratorium on live AFR 'until a legislative framework has been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established.'[33] Their concerns were, it seems, well founded. In the same month, an independent report of the Metropolitan Police Service's trial of live AFR documented identified several issues arising from the governance of the trials, pertaining to the very low number of arrests made in comparison to numbers scanned by the system; its operational use by the Met; and the legal basis relied on for the trials.[34] Perhaps owing to concern that this independent evaluation did not produce the desired results, the Metropolitan Police produced their own evaluation report, which took a more positive view of the trials and concluded that AFR will 'stop dangerous people and make London safer'.[35] The document made no reference to the independent evaluation study, and did little to address its main findings.

---

[29] K Hill, 'The secretive company that might end privacy as we know it' (*New York Times*, 18 January 2020), available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[30] R Mac et al 'Clearview's facial recognition app has been used by the Justice Department, ICE, Macy's, Walmart, and the NBA' (*Buzzfeed News,* 27 February 2020), available at: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement; A Bogle 'Documents reveal AFP's use of controversial facial recognition technology Clearview Ai' (*ABC News,* 13 July 2020), available at: https://www.abc.net.au/news/2020-07-13/afp-use-of-facial-recocognition-sofware-clearview-ai-revealed/12451554; Australian Federal Police *Clearview – Section 44 of the Privacy Act 1988 – Notice to give information and/or produce documents to the Information Commissioner* (2020), available at: https://www.afp.gov.au/sites/default/files/PDF/Disclosure-Log/02-2020.pdf.

[31] Office of the Australian Information Commissioner 'OAIC and UK's ICO open joint investigation into Clearview AI Inc.' (Media Release, 9 July 2020), available at https://www.oaic.gov.au/updates/news-and-media/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc/.

[32] Biometrics and Forensics Ethics Group *Ethical Issues Arising From the Police Use of Live Facial Recognition Technology* (February 2019).

[33] House of Commons Science and Technology Committee *The Work of the Biometrics Commissioner and the Forensic Science Regulator,* Nineteenth Report of Session 2017–19, HC 1970, 18 July 2019 (HMSO, 2019) at para 37.

[34] The Human Rights, Big Data and Technology Project *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (July 2019).

[35] Metropolitan Police Service and National Physical Laboratory *Metropolitan Police Service Live Facial Recognition Trials* (2020) p 3.

The Information Commissioner, Biometrics Commissioner and the Surveillance Camera Commissioner have all expressed concerns about the rapid rise of AFR in a policing context, too.[36] In February 2020, almost six months after the Divisional Court judgment in *Bridges* had been handed down, Lord Clement Jones sponsored a Private Members Bill, which would prohibit the use of AFR technology in public places and to provide for a review of its use.[37] At the time of writing, no date has been announced for the Bill's second reading.

Despite this widespread criticism and political resistance, the rise of AFR in policing continued apace. The South Wales Police continued to trial AFR for both live surveillance and identity verification. The Metropolitan Police have used live AFR at numerous shopping centres and public places in 2020, and several other forces are reported to have used AFR surveillance, without publicising their trials.[38] Parliament has not introduced any specific laws relating to AFR. The police have maintained that the legal basis regulating its proper operational limits lay in the DPA 2018; the Surveillance Camera Code of Practice; and relevant common law and human rights principles. As indicated above, these arguments were put to the test in the *Bridges* case, when a Divisional Court considered an application for judicial review of the legality of South Wales Police's use of AFR.[39]

3. *R (BRIDGES) V CHIEF CONSTABLE OF SOUTH WALES POLICE*

South Wales Police is the national lead on AFR, having received a £2.6 million government grant to test the technology.[40] A Cardiff resident, Mr Bridges (described as a civil liberties campaigner) had challenged the legality of SWP's general use and two particular deployments of AFR on the grounds that this was contrary to the Human Rights Act 1998, Data Protection legislation, and that the decision to implement it had not been taken in accordance with the Equality Act 2010. The Divisional Court rejected this application.

It is worth highlighting some of the dimensions of the SWP initiative to illuminate the reasons behind the Divisional Court's refusal of judicial review, and the later overturning of this decision on appeal. In April 2017, SWP began a trial of automatic AFR with subsequent national rollout in mind. The trial comprised two pilots, one of which was known as AFR Locate and the other known as AFR Identify. The judicial review proceedings concerned AFR Locate; a form of live AFR. This involves the processing of digital images of members of the public taken from live CCTV feeds, and the comparison of these images with biometric information of individuals on a watchlist compiled specifically for the purpose of the deployment of AFR. The SWP took steps to inform members of the public that AFR Locate

[36] see *ICO investigation into how the police use facial recognition technology in public places* 31 October 2019, https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf ; https://www.gov.uk/government/news/automated-facial-recognition; https://videosurveillance.blog.gov.uk/2019/11/01/regulating-law-enforcement-use-of-automatic-facial-recognition/

[37] Automated Facial Recognition Technology (Moratorium and Review) Bill 2019–2021.

[38] O Williams 'The Met and NCA "used Clearview AI's facial recognition database"' (*New Statesman,* 28 February 2020), available at: https://tech.newstatesman.com/security/the-met-and-nca-used-clearview-ais-facial-recognition-database.

[39] *Bridges* (Divisional Court), above n 23.

[40] 'Police transformation fund: successful bids 2016 to 2017' (Web Page), available at: https://www.gov.uk/government/publications/police-transformation-fund-successful-bids-2016-to-2017.

was being used at a particular event or area by posting on social media and putting signs up in the vicinity of the trial.

In terms of human rights, the Divisional Court concluded that while the use of AFR Locate engaged the ECHR Article 8 (privacy) rights of the members of the public whose images were taken and processed, there was no violation of Article 8 as the SWP's use of AFR was 'in accordance with the law' and was 'necessary in a democratic society', and in pursuit of the legitimate aim of preventing or detecting crime, for the purposes of Article 8(2). On the legality point, AFR use was deemed to be within the police's common law powers so that there is currently no need to legislate to permit its use and it was not *ultra vires*, at least as practised in the SWP trials. Moreover, those actions were subject to adequate legal controls, contained in Data Protection legislation, statutory codes of practice, and SWP's policies. The pilots were legally justified; AFR Locate was deployed only for a limited time, and for specific and limited purposes. Furthermore, unless someone's image matched that on the watchlist, all data were deleted immediately after having been processed. The CCTV feed is retained for 31 days in accordance with the standard CCTV retention period, and data associated with a match is retained within AFR Locate for up to 24 hours. In its necessity analysis, the Divisional Court found that the benefits of live AFR were potentially great, as serious offenders might be apprehended, and the impact on Mr Bridges was relatively minor as he was not stopped by the police, and so the use of AFR was proportionate under Article 8(2).

As for the data protection claims, the Court determined that the collection and processing by SWP of images of members of the public constituted collecting and processing of their personal data, notwithstanding that they might not be identifiable by name. Such processing of personal data was deemed to be lawful and to comply with the conditions in the DPA 2018. The Court was also satisfied that SWP had complied with the requirements of the public sector equality duty.

Mr Bridges sought leave to appeal the Divisional Court's decision on the following five grounds:

1. The Divisional Court erred in concluding that the interference with the Appellant's Article 8 rights occasioned by SWP's use of AFR was 'in accordance with the law' for the purposes of Article 8(2) ECHR.
2. The Court made an error of law in assessing whether SWP's use of AFR constituted a proportionate interference with the appellant's Article 8 rights.
3. The Divisional Court erred in holding that SWP's Data Protection Impact Assessment complied with the DPA 2018, s 64.
4. the Divisional Court erred in declining to reach a conclusion on whether SWP has in place an appropriate policy document within the meaning of the DPA 2018, s 42 (taken with s 35(5)), which is a condition precedent for lawful data processing.
5. the Divisional Court made an error of law in concluding that SWP has complied with the Public Sector Equality Duty the Equality Act 2010, s 149, given that its approach to the equalities implications of AFR is 'demonstrably flawed' as it failed to recognise the risk of indirect discrimination.[41]

[41] *R (Bridges) v SWP* (2020) EWCA Civ 1058 at [53].

On the first ground, the Court of Appeal ruled that the Divisional Court did err in its finding that the measures were 'in accordance with the law'. The Court of Appeal did not revisit the issue of whether or not the use of AFR was *ultra vires* the SWP, holding that the police had long used overt surveillance techniques such as overt photography that were 'undoubtedly' in accordance with the law.[42] Instead, the Court engaged in a holistic analysis of whether the framework governing the SWP's use of live AFR was reasonably accessible and predictable in its application,[43] and sufficiently prescribed to guard against 'overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'.[44]

The Court of Appeal rejected the contention that for the police to use AFR they needed some statutory authorisation, but accepted, applying a relativist approach, that more would be required by way of safeguards for AFR than for overt photography as the former was a novel technology that involved the automated processing of sensitive data.[45] However, unlike the Divisional Court, the Court of Appeal was not satisfied that the SWP's use of live AFR was sufficiently regulated by the combination of the DPA 2018, the Surveillance Camera Code of Practice and SWP's local policies. In particular, the legal framework left too much discretion in the hands of individual officers to determine who was to be placed on the watchlist, and where AFR could be deployed.[46] Thus, the framework did not sufficiently set out the terms on which discretionary powers in these areas could be exercised and for that reason they did not have the necessary quality of law. The Court held that a police force's local policies could constitute relevant law in this context, provided they were published and would not leave too much discretion to individual officers. This finding is significant. In short, if SWP were to amend their own policies in such a way that the criteria for (i) who could be put on a watchlist, and (ii) where AFR could be used, were more narrowly circumscribed, this could be all that is needed to satisfy the 'in accordance with the law' limb of article 8(2).

The appeal did not succeed on the second ground. Here, the Court held that the SWP's use of AFR was a proportionate interference with Article 8 rights, and as such was 'necessary' and 'in pursuit of a legitimate aim' under Article 8(2). The appellant submitted that the Divisional Court fell into error as a matter of approach when addressing the question of proportionality, because it conducted a weighing exercise with one side being the actual and anticipated benefits of AFR Locate and the other side being the impact of AFR deployment on the appellant. The appellant argued that 'as a matter of common sense', account needs to be taken of the interference with the Article 8 rights not only of the particular appellant but all other members of the public in the vicinity of SWP's AFR deployments.[47] The Court of Appeal rejected this argument as the focus of the appeal was the impact upon the appellant alone, and, in any event, the impact on the Article 8 rights of other members of the public was as negligible as it was on the appellant. In the Court's words, 'An impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication.'[48]

---

[42] Ibid at [84].
[43] Here, *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9 at [11]–[14] per Lord Sumption was cited with approval.
[44] *Beghal v Director of Public Prosecutions* [2016] AC 88 at [31] and [32] per Lord Hughes.
[45] *Bridges*, above n 44, at [85]–[90].
[46] Ibid, at [96].
[47] Ibid, at [136].
[48] Ibid, at [143].

On ground three, the Divisional Court erred in finding that SWP provided an adequate 'data protection impact assessment' (DPIA) as required by DPA 2018, s 64. The 'inevitable consequence' of the data protection impact assessment being written on the basis that Article 8 is not infringed is that it failed to adequately assess the risks to the rights and freedoms of data subjects or include the measures envisaged to address the risks arising from those deficiencies as required by Data Protection Act 2018, s 64(3)(b) and (c). However, on the fourth ground the Court of Appeal held that it was 'entirely appropriate' for the Divisional Court not to reach a conclusion as to whether SWP had in place an 'appropriate policy document' within the meaning of DPA 2018, s 42, as the deployments at issue took place before the DPA 2018 was enacted.[49]

Finally, the appeal succeeded on the fifth ground. The Court of Appeal held that the SWP never had due regard to the need to eliminate discrimination on the basis of sex and race. The Court of Appeal found that, whether or not the facial recognition software used by SWP is biased and creates a greater risk of false identifications among certain demographic groups, the police breached their positive duty to have due regard to the need to eliminate such discrimination; the 'SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex.'[50]

This issue of bias is contentious. It is clear that AFR varies in terms of accuracy and reliability in matching individuals to images, depending on gender, age, skin colour, etc, and such embedded bases may compound existing biases in policing. The National Institute of Standards and Technology (NIST), a subgroup of the US Federal Department of Commerce, has provided technical evaluation of over 100 commercially available facial recognition algorithms as part of its 'Facial Recognition Vendor Tests' (FRVT). They measure the accuracy of facial recognition software algorithms in 'one-to-one' (image verification) and 'one-to-many' (database search) contexts. The performance of face recognition systems can vary relative to the gender, ethnicity and age of the individuals targeted.[51] NIST's FRVT Part 3 focused specifically on demographic effects on the performance of 189 commercially available facial recognition algorithms. It found that many of the algorithms varied in performance across different demographic groups, and that the part of the world in which the algorithm was developed could have a significant impact on its performance.[52] For example, algorithms developed in the United States tend to have the high false positive rates for West and East African and East Asian people in one-to-one matching, whereas for a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces.[53] For 'one-to-many' matching, the test found that African American females were subject to high rates of false positives. This is significant because a false positive match on a 'one-to-many'

[49] Ibid, at [161].
[50] Ibid, at [199].
[51] See above note 23. J Buolamwini and T Gebru, 'Gender shades: intersectional accuracy disparities in commercial gender classification' (Conference Paper, Conference on Fairness, Accountability, and Transparency, 2018) 2; J Buolamwini, 'Response: racial and gender bias in Amazon Rekognition — commercial AI system for analyzing faces' *Medium* (25 January 2019), available at: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.
[52] National Institute of Standards and Technology *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (No 8280, 2019).
[53] Ibid, 2.

search could put an individual at risk of being subject to scrutiny by authorities as a result of an incorrect match against a database. The Court of Appeal's finding on this fifth ground is significant and welcome; it will have implications stretching to the use by public authorities of algorithmic technologies generally. The Court of Appeal has made clear that public authorities have a positive duty to take measures, such as independent verification, to ensure that the technologies they use for processing sensitive personal data do not produce unacceptable demographic bias.

Bridges was the first ever legal challenge to the use of AFR. The Court of Appeal has underlined that the police do not enjoy boundless discretion to deploy biometric surveillance on the general public as they traverse publicly accessible space. In the aftermath of the Court of Appeal's decision in *Bridges*, the response of both the Metropolitan Police and the South Wales Police seems to suggest that judgment will not serve as the end of a legal saga on the limits of police AFR surveillance. South Wales Police has indicated that it will not appeal the Court of Appeal's decision and in published comments following the judgement, stated:

> There is nothing in the Court of Appeal judgment that fundamentally undermines the use of facial recognition to protect the public. This judgement will only strengthen the work which is already underway to ensure that the operational policies we have in place can withstand robust legal challenge and public scrutiny.[54]

In its own reaction, the MPS gave clear indication that the judgment would not present significant obstacles to its own use of live AFR, emphasising that its own live AFR operations could be distinguished from the SWP's trials; the main differences being that the MPS's use of this technology '… is intelligence-led, and focused on helping tackle serious crime, including serious violence, gun and knife crime, child sexual exploitation and helping protect the vulnerable.' As well as being more targeted in its use, the MPS also claimed that its AFR operations are supported by its own bespoke guiding policy documents and 'the latest accurate algorithm'.[55]

The police commitment to use AFR has seemingly held firm. The police are considering how, and not whether, their AFR operations and policies can be brought into alignment with the requirements of law post-*Bridges*. This should not be too surprising, given that both SWP and the MPS have invested considerable resources in their AFR infrastructure to date.

Although the outcome of *Bridges* may appear at first glance to deal a heavy blow to the police's ambitions to continue to develop and deploy AFR, owing to the way the case was decided, the police may be able to make their AFR operations legally compliant through minor procedural amendments. For example, the Court of Appeal left open the possibility that an internal police policy document could be brought into accordance with the law for Article 8 purposes if it limited the discretion of individual officers as to who can go on a watchlist and where AFR can be used. The SWP could clear this low hurdle by making tweaks to its own internal policies, despite the absence of a positive legal basis for the police use of AFR beyond general common law powers. The Court of Appeal also found that the use of AFR by SWP was proportionate in

[54] South Wales Police 'Response to the Court of Appeal judgment on the use of facial recognition technology' (Media Release, 11 August 2020), available at: https://www.south-wales.police.uk/en/newsroom/response-to-the-court-of-appeal-judgment-on-the-use-of-facial-recognition-technology/

[55] Metropolitan Police 'Live Facial Recognition' (Web Page), available at: https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

the face of reasoned doubts about its operational utility and lingering concerns about the human rights implications of scanning hundreds of thousands of people to yield comparatively few arrests.[56]

In what follows, we assess the state of the regulation of police AFR surveillance under English law, following the *Bridges* judgment. Building on our prior work regarding the threats posed to human rights by AFR surveillance, and English law's response to the use by police of this technology,[57] and drawing on the experience of other jurisdictions and relevant policing jurisprudence and literature, we examine the 'key moments' in the *Bridges* judgments, where the legal conditions necessary for the continuing expansion of experimental police surveillance have been embedded in the English legal framework by the senior courts. Through this analysis, we suggest that this framework of broad, overarching safeguards still opens up vast operational discretion for the police to set the limits of 'lawful' use of an intrusive surveillance technology; the human rights and data protection framework functioning less as a barrier to government power, and more as a tool of *post hoc* legitimation, and an instrument of its expansion without prior democratic approval.[58] Thus, although the regulatory framework for police AFR surveillance is based on a discourse of respecting human rights, this discourse serves to provide cover for the expansion of pervasive surveillance in practice.[59]

4. THE LEGAL BASIS FOR POLICE AFR SURVEILLANCE

Unlike in several continental European jurisdictions, there is no exhaustive code of criminal procedure providing explicit textual basis for the exercise of potentially coercive police powers.[60] Instead, the legal basis for the exercise of police power in England and Wales is multifaceted; it consists of statute, delegated legislation, and common law with each piece of this moveable mosaic shifting into its proper place depending on the power under exercise. For example, to compile a watchlist of images of offenders, the police will typically be able to rely on explicit statutory powers to collect and use of custody images, such as those contained in s 64A of the Police and Criminal Evidence Act 1984. Other statutes, such as the Data Protection Act 2018 and the Protection of Freedoms Act 2012 regulate aspects of AFR use by public and private authorities, providing for public notification requirements and retention limits, for example. However, under English law there is no explicit textual provision for the police use of AFR. Without explicit authorisation for the use of AFR from the legislature in the form of an authorising statutory provision, the police must find some other explicit or implicit power or liberty supporting their use of this technology.

---

[56] According to the MPS's own data, approximately 180,000 people were scanned across its 10 trials of AFR, leading to 27 people being engaged following an alert and just 9 arrests or other actions being taken based on an AFR match; Metropolitan Police Service and National Physical Laboratory *Metropolitan Police Service Live Facial Recognition Trials* (2020) p 3.

[57] See Lynch et al, above n 22; above n 23.

[58] R Lippert and K Walby, 'Governing through privacy: authoritarian liberalism, law, and privacy knowledge' (2016) 12 Law, Culture and the Humanities 329 at 331.

[59] For a broader discussion of how human rights law and discourse can accommodate authoritarian government practices see C Hamilton and R Lippert, 'Governing through human rights in counter-terrorism: proofing, problematization and securitization' (2020) 28 Critical Criminology 127.

[60] P Roberts, 'Law and criminal investigation' in T Newburn, T Williamson, and A Wright (eds) *Handbook of Criminal Investigation* (Oxon: Willan, 2007) p 97.

For many of their day-to-day activities, the constable can rely on the same residual liberties that all citizens enjoy to do anything that is not expressly forbidden by law.[61] This residual liberty has its roots in the historical evolution of the police constable as a 'citizen in uniform' patrolling the streets for the benefit, and with the consent, of *his* fellow citizens.[62] In *Malone v Metropolitan Police Commissioner,* this residual liberty was held to extend very far indeed, covering the activities of the Post Office when they, acting on the request of the Metropolitan Police, tapped the telephone line of the plaintiff. Despite the absence of any statutory basis for the tapping of the telephone line by the authorities at the time, Sir Robert Megarry VC held that the tapping was not unlawful, as there was no positive legal right to immunity from this activity, observing:

> England, it may be said, is not a country where everything is forbidden except what is expressly permitted: it is a country where everything is permitted except what is expressly forbidden.[63]

The 'citizen in uniform' conception of the constable and the extent of the residual liberty he or she enjoys are both contestable,[64] but it is clear that this residual liberty no longer extends to cover intrusive and covert surveillance activities such as wiretaps and other communication interceptions. In *Malone v United Kingdom*, the European Court of Human Rights (ECtHR) held that the UK Government's reliance on this residual liberty did not satisfy the 'in accordance with the law' limb of Article 8(2).[65] By the time the judgment was delivered, the Government had already placed the regulation of public authority wiretapping on a statutory footing in the Interception of Communications Act 1985.

The idea that the police could depend on this residual liberty to engage in overt surveillance, such as recording and monitoring individuals in public spaces, has persisted. In *Murray v United Kingdom*, the first applicant was detained by the British Army in Belfast during the Northern Ireland conflict and taken to a screening centre. She argued, *inter alia,* that her Article 8 rights had been violated as she was photographed by the British Army, without her knowledge and consent, and the photographs were kept on record along with personal details about her, her family and her home. The domestic courts had dismissed her claim that the taking and retention of her photograph in these circumstances was in any way actionable, with the Court of Appeal in Northern Ireland finding:

> The act of taking the photograph involved nothing in the nature of a physical assault. Whether such an act would constitute an invasion of privacy so as to be actionable in the United States is irrelevant, because the [first applicant] can only recover damages if it

---

[61] *Malone v Metropolitan Police Commissioner* [1979] Ch 344 at p 357; *Collins v Wilcock* [1984] 1 WLR 1172 at p 1178.

[62] See Home Office, *Royal Commission on Police Powers and Procedure* (Command Paper 3297 1929) 6. As Roberts describes: 'Just as you or I can stop a stranger in the street to request directions, to ask the time, to solicit a donation to charity or for any other lawful purpose, the police are similarly entitled to stop a stranger in the street and ask him or her what he or she is doing, whether he or she has seen anything suspicious, where he or she lives,' P Roberts, 'Law and Criminal Investigation' in T Newburn, T Williamson, and A Wright (eds) *Handbook of Criminal Investigation* (Oxon: Willan, 2007) p 97.

[63] *Malone v Metropolitan Police Commissioner* [1979] Ch 344 at p 357.

[64] See generally *R v Somerset County Council, ex p Fewings* [1995] 1 All ER 513. For a fuller discussion of the historical roots of this conception of the constable and the residual liberty of police officers to do everything 'except what is expressly forbidden', see V Aston, 'Conceptualising surveillance harms in the context of political protest: privacy, autonomy and freedom of assembly' (PhD Thesis, University of East Anglia, 2019).

[65] See *Malone v United Kingdom* (1984) 7 EHRR 14 at [79].

> amounts to a tort falling within one of the recognised branches of the law on the topic. According to the common law there is no remedy if someone takes a photograph of another against his will.[66]

Thus, the actions of the British Army were said to be lawful because they were not legally forbidden. The ECtHR rejected the applicant's contention that the measures lacked a legal basis such as is required for the measures to be 'in accordance with the law' under Article 8(2). The Strasbourg Court ruled that the common law provided sufficient domestic legal basis.[67]

Then in *R (Wood) v Commissioner of Police for the Metropolis*, the Court of Appeal considered the legal basis for overt police photography surveillance.[68] The claimant - a political campaigner - was photographed by the police at a protest outside the Annual General Meeting of a company connected to the arms trade. A majority of the Court held that the police had violated the claimant's Article 8 rights because the collection and retention of the images was disproportionate in the circumstances. The Court did not reach a decisive view on whether the common law provided adequate legal basis for the activities of the police to be 'in accordance with the law'. Although *obiter*, Laws LJ observed, 'the requirement of legality is in my judgment satisfied by the general common law power referred to in *Murray*'.[69]

This line of authority seems to indicate that the police do not require a positive legal power to engage in overt surveillance operations. However, in its more recent case law the ECtHR has been more exacting in its analysis of the quality of the legal basis underpinning surveillance measures, including the use of photography.[70] It is noteworthy in this regard that *Murray v United Kingdom* predates the enactment of the Human Rights Act 1998 which, under s 6, places a direct obligation on the police ensure that all of their activities are compatible with Convention rights. In any event, the police use of AFR, even in public spaces, can be distinguished from the police collection and retention of photographs of the applicants in *Wood* and *Murray,* because AFR involves biometric data processing. This point was recognised by both the Divisional Court and Court of Appeal in *Bridges*.[71] It is perhaps out of sensitivity to these developments in the legal and technological landscape that the police have tended in recent challenges to their use of overt surveillance to rely on positive powers to engage in various activities in the fulfilment of their basic common law duties, to justify the use of overt surveillance technologies.[72]

---

[66] *Murray v Ministry of Defence* [1987] NI 219, as quoted in *Murray v United Kingdom* (1995) 19 EHRR 193 at [30].
[67] *Murray v United Kingdom* (1995) 19 EHRR 193 at [88].
[68] *R (on the application of Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123.
[69] *R (on the application of Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123 at [54].
[70] See for example *Peck v United Kingdom* (2003) 36 EHRR 41; *S and Marper v United Kingdom* [2008] ECHR 1581; *MM v United Kingdom* [2012] ECHR 1906.
[71] *Bridges*, above n 44, at [85].
[72] See for example Metropolitan Police Service *Live Facial Recognition: Legal Mandate* (Version 1-01, 2020) para 2.2. Aston engages in detail with the seeming juridical tension between these two competing conceptions of the common law, and elucidates the difficulty in either of them providing an adequate legal basis for overt surveillance in the related context of overt police photography of public protests. See V Aston, 'Conceptualising surveillance harms in the context of political protest: privacy, autonomy and freedom of assembly' (PhD Thesis, University of East Anglia, 2019).

In *Bridges*, the Divisional Court rejected the claimant's contention that the police could not rely on their common law powers to use AFR and, as such, the use of AFR was *ultra vires* the SWP. Haddon-Cave LJ and Swift J relied on the following passage from *Rice v Connolly*:

> [I]t is part of the obligations and duties of a police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal damage. There is no exhaustive definition of the powers and obligations of the police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice.[73]

Drawing on *Woo*d and the Supreme Court judgment in *R (Catt) v Association of Chief Police Officer,* the Divisional Court held that this general power of the police covers the use, retention, and disclosure of imagery of individuals for any of the duties articulated in *Rice*.[74] In *Catt*, the applicant unsuccessfully argued that the retention by police of information about his attendance at several protests against the arms trade, which included written notes of his activities and a photograph, violated his Article 8 rights. Lord Sumption, in the majority, held that the power of the police to engage in surveillance of this kind lay not in the residual liberty of all citizens to do anything that is not forbidden, but rather in the general common law powers of the police officer to fulfil his basic duties: 'At common law the police have the power to obtain and store information for policing purposes, ie broadly speaking for the maintenance of public order and the prevention and detection of crime.'[75]

These powers, in Lord Sumption's view, did not extend to cover what he described as 'intrusive' methods of obtaining information, such as entry upon private property or acts of physical coercion, that are normally regulated by statute or other more narrowly prescribed sources. However, they were 'amply sufficient' to cover the obtaining and storage of photographs.[76] On this basis, the Divisional Court in *Bridges* classified live AFR as 'non-intrusive' and thus falling within the scope of the common law powers of the police. The Divisional Court ruled that the distinction turned on whether there was a physical intrusion with a person's rights vis-à-vis his or her home or interference with his or her bodily integrity.[77] The Court of Appeal upheld this aspect of the Divisional Court's ruling, citing Lord Sumption's observations in *Catt* with approval. The issue for the Court of Appeal was not that there was no adequate domestic legal basis providing for the use of AFR, but rather that this basis did not meet the quality of law requirements to be 'in accordance with the law'.[78] It seems that only forms of 'physical' intrusion, such as DNA sampling and bugging private property, fall beyond the scope of the common law powers of the police, thus requiring a more narrowly prescribed legal basis.

This is a significant finding, as it permits the police to use new overt surveillance technologies like AFR operationally, without Parliament authorising this use. It puts the police collection and processing of biometric data by AFR in a separate category to other forms of biometric surveillance, such as arrestee DNA and fingerprint collection and comparison. These tend to require 'physical intrusion' and, as such, have a statutory legal basis under the Protection of

[73] *Rice v Connolly* [1966] 2 QB 414 at 419.
[74] *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 at para 7.
[75] Ibid.
[76] Ibid.
[77] *Bridges* (Divisional Court), above n 23, at [74].
[78] *Bridges*, above n 44, at [77], [91].

Freedoms Act 2012. The effect of the Divisional Court's interpretation of these cases is that statutes are only relevant in so far as they place limitations on how AFR is used by the police. Thus, the police are free to trial and use these new technologies in the absence of the democratic mandate that legislation passed by Parliament provides. If this is the case, there is no need for police AFR use to be approved by our elected representatives, usually following robust debate on the implications this use, and consideration of expert evidence scrutinised by Select Committees. The decision to use AFR is a matter for police to decide for themselves; their discretion on this matter is fettered only by the limits of their common law powers which, as the Court in *Bridges* acknowledged, are expressed in 'very broad terms'.[79] It is noteworthy that in *Catt v United Kingdom*, the ECtHR expressed concern that the collection and retention by police of personal information taken from public space in that case 'did not have a clearer and more coherent legal base' before concluding that the retention violated Article 8 ECHR.[80]

That said, it is difficult to fault the Divisional Court and Court of Appeal's interpretation of recent domestic authorities in *Wood* and *Catt,* which, as a matter of *stare decisis,* were binding on them in *Bridges.* These authorities do suggest that the general common law powers of the police set out in *Rice* extend to the collection, use, retention and dissemination of facial images. The problem is that, in interpreting the common law powers of the police so broadly, these authorities may have sent the law down a wrong path.

There is clear domestic authority for Lord Sumption's observation in *Catt* that physical acts which would otherwise constitute a technical assault or trespass fall far outside the scope of the common law powers of police.[81] However, it does not necessarily follow that the powers conferred upon police by their common law duties extend to cover all acts that are not 'physically' intrusive in the sense described in *Bridges*. For example, in *Rice,* the appellant successfully argued that the offence of obstruction of justice was not made out in circumstances where he merely refused to provide his name or other assistance to a police constable in the course of his investigation into a series of breaking offences. Lord Parker CJ held that police constables have a duty to take steps which appear necessary to prevent and detect crime. However, as Aston notes, this finding was 'categorical'; the power of the constable did not extend to taking all steps he considered necessary for the prevention or detection of crime.[82] Indeed, Lord Parker CJ held that there are clear limits on the common law power (beyond those that interfere with the individual's physical home or bodily integrity); one being that citizens are not under a general legal duty to assist the police by providing them with information, and police cannot rely on their common law powers to demand such assistance. This was the unambiguous ratio of *Rice*.

We submit that other forms of non-physical coercion of citizens (such as verbally badgering or harassing an individual in the street) would also fall beyond the common law powers of the police, even if they involve no physical restriction of the individual's movement. None of the judgments of senior courts prior to *Bridges* drew the boundary of the common law powers so bluntly. Historically, domestic courts have tended to focus on whether the conduct of a police

[79] *Bridges* (Divisional Court), above n 23, at [73].
[80] *Catt v United Kingdom* App no 43514/15 (ECHR, 24 January 2019) at [98].
[81] See for example *Davis v Lisle* [1936] 2 KB 434; *Kenlin v Gardiner* [1967] 2 QB 510; *Walker v Commissioner of Police of the Metropolis* [2014] EWCA Civ 897.
[82] V Aston, 'Conceptualising surveillance harms in the context of political protest: privacy, autonomy and freedom of assembly' (PhD Thesis, University of East Anglia, 2019) 77.

officer constitutes a significant interference with the individual's liberty or property generally, and not on the existence of physical contact. Thus, in the famous case of *Collins v Wilcock*, Goff LJ held

> A police officer has no power to require a man to answer him, though he has the advantage of authority, enhanced as it is by the uniform which the state provides and requires him to wear, in seeking a response to his inquiry. What is not permitted, however, is the unlawful use of force or the unlawful threat, actual or implicit, to use force.[83]

Here, the Court recognises that, as well as physical intrusions, excessive demands to answer questions, including the use of actual or implicit threats fall outside of the common law powers. Indeed, some forms of physical touching will fall *within* the police common law powers, as in *Donnelly v Jackman,* where a police officer repeatedly tapped a man on the shoulder in order to get his attention for the purpose of making enquiries about an offence which the officer had cause to believe the defendant might have committed.[84] Even though this case involved making physical contact with the defendant, the Court focused on the degree of intrusion into the person's liberty and not on whether the type of intrusion involved trespass onto his physical realm. As Talbot J stated, 'it is not every trivial interference with a citizen's liberty that amounts to a course of conduct sufficient to take the officer out of the course of his duties.'[85]

The focus in *Donnelly,* on the significance of the intrusion with the person's liberty to use public space unmolested, seems better equipped for the information age than an arbitrary focus on whether the means used by police to obtain personal information occasioned physical contact. It is one thing to hold that the common law power to prevent crime and bring offenders to justice is good enough for the police to ask for identifying particulars of a person seen in the vicinity of reported criminality (even though the person may be under no legal obligation to comply with the request). It is quite another for this same power to support the use of myriad biometric and/or algorithmic technologies, which facilitate the use and collection of ever-more sensitive personal information by public authorities. AFR enmeshes physical and informational forms of surveillance by collecting information from the physical body of the person (albeit without occasioning physical contact) and breaking this down into an information structure, which can then be processed. The distinction for fleshing out the scope of the common law powers of the police, between physical and informational intrusions, does not seem to recognise that physical contact is a poor barometer for gauging the intrusiveness of a surveillance measure. The common law powers of the police enunciated in *Rice* have been extended too far.

(a) Proportionality, Balancing and 'Tick-Box' Human Rights Protection

One significant and unresolved issue with the English legal framework as it relates to AFR is that it leaves it largely to the police to decide whether the use of AFR (and thus further biometric technologies as they emerge) is 'proportionate and necessary', according to the precepts of the common law necessity test; Article 8(2); and the DPA and so on. The Appeal Court in *Bridges* considered the question of proportionality, and noted that, strictly speaking,

---

[83] *Collins v Wilcock* [1984] 1 WLR 1172 at 1178; See also *R v Waterfield* [1964] 1 QB 164 at 170 per Ashworth J.
[84] *Donnelly v Jackman* (1970) 1 WLR 562.
[85] Ibid, at 565.

it was unnecessary to do so.[86] Regrettably, this assessment was formalistic, not internally consistent, and unduly brief.

As indicated in the account of the case above, Mr Bridges submitted that the Divisional Court had erred when examining the 'cost' side of proportionality by taking into account the impact of AFR on him alone, and that 'as a matter of common sense' account should be taken of the interference with the Article 8 rights of all other members of the public present at the two deployments also.[87] This contention was rejected by the Appeal Court, which held that the challenge was to a 'very specific deployment of AFR Locate on two particular occasions'. To come to this conclusion, it drew on the precise terms of the Statement of Facts and Grounds that this Appellant's Article 8 rights had been violated. It is regrettable that the ground on proportionality was not framed in more general terms. Indeed, both the Court of Appeal and the Divisional Court themselves framed the appeal as a review of the legality of SWP's 'ongoing' trial of AFR. Moreover, one can question how the proportionality of future use could be assessed adequately through reference to the impact it has on Mr Bridges solely. We suggest a wider lens should have been adopted in terms of scrutinising proportionality, given the impact on other individuals in these deployments and beyond.

The Court of Appeal differentiated *Bridges* from challenges to a 'general measure, for example a policy or even a piece of legislation', such as in *Tigere* where the Supreme Court considered eligibility for student loans for English residents.[88] In such challenges to a 'general measure', it may be appropriate for the Court to assess the balance between the impact on every person who is affected by the measure and the interests of the community.[89] That was not the interpretation in *Bridges*. The Court could have considered this use of AFR a 'general measure', affecting as it did anyone in particular public spaces in Cardiff during certain times. That said, States are afforded a wider margin of appreciation when it comes to measures of general economic or social strategy,[90] so this would not affect the ultimate determination. Even without such an interpretation, the Court could have considered more fully the intrusion on every person subject to the deployment of the technology, as well as on the public *en masse*.

As well as limiting the breadth of the impact, the level of the perceived intrusion was also downplayed by the Court. The effect on members of the public who were in an analogous situation to Bridges was 'as negligible as the impact on the Appellant's Article 8 rights', and this impact of 'very little weight cannot become weightier simply because other people were also affected'. The Court stated that this was not a question of simple multiplication, but rather an exercise of judgement.[91] There is little elaboration of what this judgement entailed. Moreover, in terms of consistency, it is hard to reconcile this statement about negligible impact with the holding of the Divisional Court that Article 8 was engaged by AFR technology, the

[86] *Bridges*, above n 44, at [131].
[87] Ibid, at [136].
[88] Ibid, at [140], citing *R (Tigere) v Secretary of State for Business, Innovation and Skills* [2015] UKSC 57.
[89] Ibid.
[90] *Stec v United Kingdom* 65731/01 (2006) 43 EHRR 47 at [52]: 'a wide margin is usually allowed to the State under the Convention when it comes to general measures of economic or social strategy. Because of their direct knowledge of their society and its needs … the Court will generally respect the legislature's policy choice unless it is "manifestly without reasonable foundation"'; J Meers 'Problems with the "manifestly without reasonable foundation" test' (2020) 27 Journal Social Security Law 12 criticises domestic courts for transposing the 'manifestly without reasonable foundation' test into domestic cases pertaining to general measures of economic/social policy, instead of doing a full proportionality analysis, effectively setting a very low bar for legislators.
[91] *Bridges*, above n 44, at [143].

comparison with fingerprints and DNA, and the description that AFR enables the extraction of unique information and identifiers of 'an intrinsically private character'.[92] The public visibility of a person's face was not regarded as detracting from this, and Article 8 was engaged even though retention of the data was momentary. Furthermore, the Court of Appeal approved one of the grounds of appeal which stated that the DPIA had proceeded incorrectly on the basis that Article 8 was not engaged nor 'more accurately was not infringed'.[93]

It is difficult to see how Article 8 could be infringed just negligibly by AFR. That said, this is a common approach of domestic courts in surveillance cases, whereby the interference is characterised as minor or of negligible impact, before the benefits are trumpeted.[94] Courts seem to overlook the reality of overt and biometric surveillance as a preventive policing strategy geared towards the effective management of populations, and instead focus on individual (and physically intrusive) liberty restriction. This is a partial and questionable approach. This approach also seems out of step with ECtHR jurisprudence, which has consistently held that the recording and processing of an individual's photographic data is protected by Article 8. In *Reklos v Greece*, the ECtHR held

> A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.[95]

The ECtHR has held that where a record of an individual's image is generated from CCTV cameras monitoring publicly accessible space, and retained by a public authority,[96] this can engage Article 8. AFR surveillance goes further than merely collecting and storing photographic images through CCTV surveillance as it involves the biometric processing of the facial geometry of those scanned. This enables public authorities to subject those who traverse public space to an automated identification process in real-time, without their knowledge or consent. Thus, AFR surveillance enables the police to go further in transgressing social norms governing the flow of information about individuals as they occupy public space than CCTV surveillance or other forms of overt photography.[97]

The concept of proportionality is embedded in human rights jurisprudence and discourse, though it is not uncontroversial.[98] In this specific instance, the analysis in *Bridges* on proportionality overall was perfunctory, and did not really come close to grappling with the politically contentious issues at the heart of the debate on AFR, and its wider social effects, beyond the impact on the individual claimant. It might well be argued that a court is not best placed to engage in this sort of in-depth normative analysis, which is a fair remark. But, as Parliament has declined to regulate AFR in any meaningful way, and indeed is not required to do so, the decision of when and where AFR is proportionate is left largely in the hands of the

---

[92] Ibid, at [36] citing HC [57]-[59].
[93] Ibid, at [152].
[94] Eg *Catt v Metropolitan Police Commissioner*; *R (RMC and FJ) v Metropolitan Police Commissioner* [2012] EWHC 1681.
[95] *Reklos v Greece* [2009] EMLR 16 at [300].
[96] *PG and JH v United Kingdom* (2001) 46 EHRR 127 at [57].
[97] above n 23.
[98] See for example S Tsakyrakis 'Proportionality: an assault on human rights?' (2010) 7 International Journal Constitutional Law 468; M Khosla 'Proportionality: an assault on human rights? A reply' (2010) 8 International Journal Constitutional Law 298.

police, who are institutionally ill-suited to striking a fair balance between crime control and human rights impacts. Although process-based judicial review aims to harness the legislature and police to broader HR principles, this is inadequate because it entails a *post hoc* consideration where the role of the court is to engage in a limited review of AFR surveillance, grounded in broad common law compliance and a brief necessity analysis, and not to draft legislation on the appropriate limits of AFR.

Moreover, the full spectrum of harms cannot be captured through orthodox legal analytical lenses regarding human rights and data protection, which are focused on the impact on individual rights against state/data controller. The impact of the police use of AFR is greater than the impact it has on any one individual subject to AFR processing. It shifts the balance of power between state, who are using the products of private companies, and the public in favour of the former. In essence, law is not enough.

(b) Some comparative insights

Other jurisdictions, like Scotland and New Zealand, are proceeding with more caution in this context, in contrast to England and Wales, Australia and the US.[99]

In New Zealand, some human rights protections applicable to AFR surveillance are less entrenched in the domestic legal framework than in England and Wales.[100] For example, individuals cannot use domestic human rights legislation to advance a judicial review of the effect of a piece of legislation or policy affecting their rights. Moreover, New Zealand's Privacy Act 2020 does not offer the same level of protection for the collection and processing of AFR data as the European's Union General Data Processing Regulation (GDPR). The Privacy Act 2020 offers a single level of protection for all personal information without distinguishing AFR as involving the processing of sensitive biometric data, and does not require that the use of AFR must be 'strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject'.[101]

Despite sharing a broad alignment with England and Wales in terms of legal structure - particularly as far as the applicability of human rights and data protection provisions to the police use of AFR is concerned - Scotland has imposed a moratorium on live AFR. While Police Scotland's 10-year strategy, *Policing 2026*, included a proposal to introduce AFR,[102] a Scottish parliamentary committee was highly critical of this plan. The Justice Sub-Committee on Policing found that the proposed live facial recognition software is known to discriminate against women and those from black, Asian and ethnic minority communities; that there is no justifiable basis for Police Scotland to invest in this technology; that prior to any decision to introduce it a robust and transparent assessment of its necessity and accuracy should be undertaken; that its potential impacts on people and communities should be understood, and overall that AFR would be a radical departure from the fundamental principle of policing by

[99] see Lynch et al, above n 22. M Mann and M Smith 'Automated facial recognition technology: recent developments and approaches to oversight' (2017) 40 University of New South Wales Law Journal 121.
[100] For further discussion of the regulation of AFR in New Zealand, see Lynch et al, above n 22.
[101] see Lynch et al, above n 22, p 74.
[102] Police Scotland and Scottish Police Authority *Policing 2026: Our 10 year strategy for policing in Scotland* (2017), available at: https://www.scotland.police.uk/spa-media/jjkpn4et/policing-2026-strategy.pdf?view=Standard.

consent.[103] A subsequent response from Police Scotland indicated that, much like in New Zealand, the police were not using live facial recognition technology currently, and had no plans to do so. Police Scotland was also clear that it would ensure safeguards are in place prior to introducing AFR, and agreed that the impact of its use should be fully understood before it is introduced.[104]

The experiences of New Zealand and Scotland serve to show that in England and Wales pervasive AFR surveillance is the product of both structural legal weakness *and* cultural permissiveness of surveillance. We endorse the approach of the Scottish Government that has emphasised the need for assessment of human rights impact prior to the introduction of any technology, not afterwards as occurred in England and Wales. Moreover, the parliamentary report's foregrounding of communities and consent to policing is key.

Such contrasting dynamics in terms of policing and politics within Great Britain are not unique. The situation in England and Wales can be seen to follow a pattern that emerged in respect of police use of DNA material, another form of biometrics, where likewise the onus was on the individual to challenge expansive laws and practices after the event. In contrast to AFR, however, the police were not pushing the boundaries of what was permitted in respect of DNA, or operating under any legal uncertainty, but rather were complying with the terms of what was deemed ultimately to be problematic legislation, in terms of human rights. So rather than a legal lacuna as regarding AFR, the law on DNA collection and retention was remarkably permissive.

In *S and Marper v United Kingdom*,[105] the ECtHR considered an Article 8(2) challenge to laws in England and Wales which permitted a non-intimate sample[106] like a mouth swab to be taken without consent from a person who had been charged with, informed that they would be reported for, or convicted of a recordable offence.[107] Such DNA samples were kept indefinitely, regardless of the outcome of the investigation or subsequent criminal trial, due to their perceived value in crime control.[108] Two people, S (a child who was acquitted) and Marper (an adult against whom proceedings were not initiated), sought judicial review of the police decision to collect and retain DNA from them, based on the existing legal framework. Their claim was unsuccessful in the High Court, whose decision was upheld by the Court of Appeal, on the basis that the risks to the individual were not great and were outweighed by the benefits of retention. Similarly, the House of Lords dismissed their appeal, finding that there was no breach of Article 8 and that if such a breach had occurred it constituted just minor interference, and that retention was proportionate to its aims.[109] (This is akin to the Court of Appeal in *Bridges*.) In contrast, the Grand Chamber in Strasbourg held that such 'blanket and indiscriminate' retention of DNA violated Article 8.[110] Unlike in *Bridges*, the issue there was

[103] Justice Sub-Committee on Policing, *Facial recognition: how policing in Scotland makes use of this technology* SP Paper 678 1st Report, 2020 (Session 5) 11 February 2020.
[104] Letter from Assistant Chief Constable Duncan Sloan to Justice Sub-Committee Convener, 8 April 2020, available at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20200410_PStoJF_Facial_Recognitio....pdf.
[105] *S and Marper v United Kingdom* [2008] ECHR 1581.
[106] See Police and Criminal Evidence Act 1984, ss 62-63.
[107] Criminal Justice Act 2003, s 10.
[108] Criminal Justice and Police Act 2001, s 64(1)A.
[109] See L Campbell 'A Rights-Based Analysis of DNA Retention: "Non-Conviction" Databases and the Liberal State' (2010) Criminal Law Review 889.
[110] *S v United Kingdom* (2009) 48 EHRR 50 at [119].

retention rather than collection and processing per se. Notably for present purposes, the European Court endorsed the Scottish approach, whereby non-conviction-based DNA retention occurred for serious suspected offences for a certain timeframe only.[111] DNA could be collected in Scotland from someone arrested and detained on suspicion of having committed an offence punishable by imprisonment, and such samples and information derived from them would be destroyed following a decision not to institute criminal proceedings or when proceedings did not end with conviction.[112] DNA retention was allowed after prosecutions which did not lead to conviction for certain sexual or violent offences only.[113]

In *Bridges*, the Court of Appeal claimed that 'the context of [*S and Marper*] is far removed from [*Bridges*]'[114]. While the context of the case itself might differ in respect of the particular sort of interference, the legislative and preceding context is comparable. So the more cautious approach of Scotland has been evidenced previously. While one could regard this as exemplifying the luxury of a smaller jurisdiction, with fewer issues of crime, this is not sustainable. Rather this embodies the impact of a more interventionist and rights-oriented Parliamentary culture, and less of a law and order discourse. The state of affairs in England and Wales demonstrates an abdication of responsibility by Westminster Government to legislate in this context, the reticence of the courts in respect of the public framing of surveillance, and the enduring agenda and institutional bias of police forces.

5. CONCLUSION

It is clear that the police enjoy a broad discretion in using automated facial recognition, as a consequence of the overlapping, implicit framework within which they operate. We argue that AFR should not be used in the absence of explicit authorisation by Parliament with full legislative process, and there needs to be ethical review *prior* to policing roll out.[115] This article has identified a series of issues of law and political culture that have led to expansive deployments of AFR in England and Wales, without due regard for its varied human rights impacts. We do not seek to resolve the appropriate content of legislation specifically. But, when thinking of possible future regulation, we might draw on the way covert surveillance is regulated.[116] In brief, this could entail legal procedures at the national level as well as the local. In terms of the former, a national statutory basis for AFR and other police algorithmic use could provide democratic mandate, and an accompanying statutory code of practice or subordinate legislation for each type of algorithmic surveillance may provide specific rules, such as limits to specific targeted persons and locations; retention limits; and requirements that guide the necessity analysis undertaken by particular forces. At the local level, independent verification/authentication of the AFR or other algorithmic systems used could uncover and address potential accuracy and discrimination issues, with perhaps the development of an

[111] Ibid, [109]–[110].
[112] Criminal Procedure (Scotland) Act 1995, s 18.
[113] Criminal Procedure (Scotland) Act 1995, s 18A (as inserted by the Police, Public Order and Criminal Justice (Scotland) Act 2006).
[114] *Bridges*, above n 44, at [65].
[115] Cf Biometrics and Forensics Ethics Group *Ethical Issues Arising From the Police Use of Live Facial Recognition Technology* (February 2019), where the pilot project had begun already.
[116] Home Office *Covert Surveillance and Property Interference: Revised Code of Practice* (August 2018), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/20180802_CSPI_code.pdf.

approved list of providers. Requirements for the independent approval and oversight of the proportionality and necessity of operation in accordance with the Code of Practice can also be incorporated into the statutory framework as appropriate, and could take the form of judicial authorisation, as in relation to search warrants.

The Divisional Court in *Bridges* opened its judgment with an astute observation: 'The algorithms of the law must keep pace with new and emerging technologies.'[117] Beyond enticing the reader in, the line captures the significance of the challenge that faces lawmakers as new technologies increase the capacity of law enforcement agencies to subject citizens to scrutiny and control. Much like a good algorithm, English law should provide a clear process; a process for determining the limits of the police's uptake of new technology that is compatible with the rule of law and our existing international human rights obligations. In particular, with each new innovation in surveillance technology, English law should stipulate clearly whether or not it is permissible for police to deploy the technology and provide guidance on the circumstances in which it is appropriate to use the technology *before* it is operationalised. Though few technical innovations can be envisaged or predicted and so legislated for in advance, what can be done is the appropriate defining and controlling of police powers. As far as AFR is concerned, the 'algorithms' of English law suffer from numerous structural deficiencies and have failed to rise to the challenge of providing adequate regulation for expansive police surveillance.

[117] *Bridges*, above n 23, at [1].