IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION (DIVISIONAL COURT)
Lord Justice Haddon-Cave and Mr Justice Swift ([2019] EWHC 2341 (Admin))

BETWEEN:

THE QUEEN
(on the application of EDWARD BRIDGES)

Appellant/Claimant

-and-

THE CHIEF CONSTABLE OF SOUTH WALES POLICE

Respondent/Defendant

-and-

THE SECRETARY OF STATE FOR THE HOME DEPARTMENT

Interested Party

APPELLANT'S REPLACEMENT SKELETON ARGUMENT
2 April 2020

Suggested pre-reading: (time estimate: 4 hours): the judgment of the Divisional Court; the skeleton arguments; the expert reports of Dr Anil Jain; the witness statements; and the Respondent's Data Protection Impact Assessment and Equality Impact Assessment.

References to the Appeal Hearing bundles: Core Bundle [**CB/tab/page**]; Supplementary Bundle [**SB/tab/page**]. References to the Judgment of the Divisional Court (which appears at [CB/12/127-193]) are given as [**J/§paragraph number**].

A. INTRODUCTION AND SUMMARY OF APPEAL

1. The Appellant seeks permission to appeal against the order of 4 September 2019 of the Divisional Court ("**DC**") by which it dismissed his application for judicial review. The DC refused an application for permission to appeal on 27 September 2019; the DC's order of 4 September extended time for filing an Appellant's Notice at the Court of Appeal until 35 days after its determination of that application.

2. At issue in this case is whether the Respondent police force's ("**SWP**") use of live automated facial recognition technology ("**AFR**") is compatible with the right to privacy under Article 8 of the European Convention on Human Rights ("**the Convention**"), data protection legislation and the Public Sector Equality Duty ("**PSED**") in section 149 of the Equality Act 2010. As the DC observed, this case raises "*novel and important issues*" [**J/§1**]

concerning a "*new and powerful technology*" whose use gives rise to "*significant civil liberties concerns*" [**J/§7**]. This is thought to be the first case in the world in which the courts have been called upon to consider the lawfulness of AFR.

3. This case is concerned with the use of what is known as live or real-time AFR. As summarised by the DC, "*AFR technology uses … digital information [captured by CCTV cameras] to isolate pictures of individual faces, extract information about facial features from those pictures, compare that information with the watchlist information [i.e., photographs of persons SWP seeks to locate], and indicate matches between faces captured through the CCTV recording and those held on the watchlist*" [**J/§25**; see also **§133**]. The DC noted the scope and power of AFR as a surveillance tool: "*by the use of AFR technology, facial biometrics can be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale*" [**J/§43**]. At the time of the hearing, SWP had used AFR on 50 occasions and may have captured the facial biometrics of approximately 500,000 faces [**J/§36**]. As the DC noted *"[t]he overwhelming majority of persons whose biometrics are captured and processed by SWP using AFR Locate are not suspected of any wrongdoing*" [**J/§36**] and it is "*reasonable to suppose … that a large number of people whose facial biometrics are captured and processed by SWP's use of AFR are unaware of this taking place*" [**J/§40**].

4. SWP's use of AFR is part of a trial before this technology is rolled-out nationally by the police [**J/§2**]. The parties recognised that it was important, therefore, for the legal regime governing AFR to be scrutinised by the court at an early stage. They have cooperated in this litigation and agreed that no costs would be sought by either side. That remains the position in the Court of Appeal. The issues raised in the case remain of profound importance. If AFR is rolled-out nationally it will change radically the way that Britain is policed. Put simply, connected to a database with the right information, AFR could be used to identify very large numbers of people in a given place at a given time (for example those present at a protest the police are monitoring). It could also track the movements of individuals as they move around the country without them knowing they were being monitored. That is because CCTV cameras (which are ubiquitous in the UK, with estimates suggesting there are half a million in London alone) can be connected to AFR systems and can then automatically, and in real-time, identify a person whose photograph is on a database. Given the proliferation of databases operated by the police and other public

authorities, the exponential increase in information held by public bodies, and the ever increasing practice of sharing that information between public bodies, it is not difficult to imagine that police forces nationally could soon (if they cannot already) have access to photographs of the vast majority of the population. It is therefore not surprising that the Information Commissioner has described AFR as "*a real step change in the way law-abiding people are monitored as they go about their daily lives*".[1] Whether the legal regime that is required to govern AFR is sufficient to protect privacy and data rights, the test applicable to proportionality, how the potentially discriminatory effect of AFR should be examined – the issues raised by the present case – are therefore of obvious significance.

5. The Appellant challenged SWP's use of AFR (i) at two given deployments (on 21 December 2017 and on 27 March 2018); and (ii) on an ongoing basis in the police area in which he resides. Before the DC, he raised five grounds of challenge, contending that: (1) SWP's use of AFR is in breach of section 6 of the Human Rights Act 1998 ("**HRA**") because it was (and is) not in accordance with the law and gave rise to disproportionate interference with Article 8 of the Convention; (2) SWP's use of AFR at the December 2017 and March 2018 deployments was in breach of section 4 of the Data Protection Act 1998 ("**DPA 1998**") (taken with the first data protection principle contained in Part 1 of Schedule 1 to that Act); (3) SWP's ongoing use of AFR is incompatible with section 35 (which requires fair and lawful processing) of the Data Protection Act 2018 ("**DPA 2018**"); (4) SWP's Data Protection Impact Assessment ("**DPIA**") does not comply with the requirements of section 64 of the DPA 2018; and (5) SWP has failed to comply with the PSED in respect of its use of AFR.

THE JUDGMENT BELOW AND A SUMMARY OF THE GROUNDS OF APPEAL

6. The DC held that SWP's use of AFR engages the Article 8 rights of anyone whose facial biometrics are captured (or who forms part of a class of people who risk having such data captured [**J/§§52; 61**]) and entails the processing of (biometric) personal data of anyone whose facial biometrics are captured [**J/§§122-125; 132-133**]. It nevertheless dismissed the claim as it found SWP's use of AFR to be in accordance with the law, proportionate and consistent with the requirements of data protection law and the PSED. It is not the

[1] https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology-and-law-enforcement/

Appellant's case that the use of live AFR by police is incapable of being lawful. His position is that, if police are to use AFR pursuant to their common law powers, (i) this must be attended by robust constraints on the exercise of this discretion so as to provide foreseeability and safeguards to ensure that the proportionality of its use can be properly assessed, (ii) there is a need for full compliance with the obligations contained in Part 3 of the DPA 2018, and (iii) the PSED must be complied with.

7. In concluding that those requirements were satisfied, the Appellant respectfully contends that the DC made a number of errors of law. He seeks permission to appeal on the following grounds:

   7.1. **Ground 1**: the DC erred in concluding that the interference with the Appellant's Article 8 rights occasioned by SWP's use of AFR was/is in accordance with the law for the purposes of Article 8(2) of the Convention.

   7.2. **Ground 2**: the DC made an error of law in assessing whether SWP's use of AFR at the December 2017 and March 2018 deployments constituted a proportionate interference with Article 8 rights. The DC failed to consider the cumulative interference with the Article 8 rights of all those whose facial biometrics were captured as part of each deployment.

   7.3. **Ground 3**: the DC was wrong to hold that SWP's DPIA complies with section 64 of the DPA 2018 in circumstances in which it is premised on significant errors of law.

   7.4. **Ground 4**: the DC erred in declining to reach a conclusion on whether SWP has in place an appropriate policy document within the meaning of section 42 of the DPA 2018 (taken with section 35(5)), which is a condition precedent for lawful data processing.

   7.5. **Ground 5**: the DC erred in holding that SWP has complied with the PSED given that its approach to the equalities implications of AFR is demonstrably flawed and based on an error of law.

B. BACKGROUND

FACTUAL BACKGROUND

8. The purpose of live AFR is to enable the user to identify, in real-time, whether someone of whom they have a digital photograph is present at a particular location. This is done by

comparing, through algorithmic analysis, the facial biometrics of persons captured by CCTV cameras to those of persons on a database containing images of persons the user is trying to locate. Facial biometrics, like DNA profiles or fingerprints, operate to enable individuals to be uniquely identified. Essentially the use of AFR is analogous to taking the fingerprints or DNA of thousands of persons (if it could be done without their knowledge, cooperation or consent) and instantaneously comparing such biometric data to that of persons whose location is being sought. Indeed, the fact AFR can be done without knowledge, cooperation or consent, and on a mass scale, in some way renders AFR a more intrusive measure of collecting biometric information. To maximise the chances of locating one or more such persons, the user needs to capture CCTV footage, and extract the facial biometrics, of as many people as possible. In principle, it would be possible to track the movements of any given person on the database wherever the user had CCTV linked to an AFR system. It therefore becomes possible to track people's movement around the country at any location at which there is a CCTV camera. It is also possible for a user to identify a very large number of people present in a particular place, provided that they had a database containing their images. A summary (agreed by the parties) of how AFR functions is set out in the DC's judgment [**J/§§23-25**]. The Court is also referred to the First Expert Report of Dr Anil Jain, a leading expert in biometric recognition technology, which contains a more technical description of how AFR systems work [**SB/11/117-120**].

9. This claim arises from SWP's ongoing trial of AFR which started in May 2017. Since then, the force has deployed AFR (in the form of a system known as AFR Locate) on 70 occasions. The most salient features of its use are as follows. SWP compiles deployment-specific databases (known as "watchlists") containing images of persons they are seeking to locate. To date these have primarily been persons sought on warrants in the force's area and suspects but also people of interest for intelligence purposes. As set out further below, there is no restriction in any legal provision or code of practice on who can be placed on a watchlist and for what purposes AFR can be used by the police to monitor anyone whose whereabouts they wish to track. SWP populates the watchlist primarily from the force's database of approximately 500,000 custody images, but again that is not a requirement prescribed by any legal provision and the police could obtain the images from any source (including the internet) or database to which they have access. SWP uses AFR in areas of high footfall and seeks to maximise the number of people whose facial biometrics are captured – this has resulted in as many as 26,174 faces being scanned in a single

deployment [**SB/19/213**]. When the system detects a match between the facial biometrics of an image on the watchlist and those of a person whose face has been captured by a mobile CCTV camera, officers intervene to ascertain whether the match is correct. SWP does not retain the facial biometric data of persons whose images are captured on CCTV but do not generate a match.

10. The Appellant does not know whether SWP or other police forces would stop and question someone on the basis of their having taken steps to avoid AFR cameras by, for example, covering their face as they pass. It is not clear whether the police may treat such action as constituting the offence of obstructing a police officer under section 89(2) of the Police Act 1996. If this were the case, it would have obvious implications for the intrusiveness of AFR as it would essentially compel the providing of biometric data.

11. The Appellant was present on two occasions on which SWP was using AFR: on 21 December 2017 on Queen St, Cardiff, and on 27 March 2018, at a lawful protest outside the Motorpoint Arena (which was hosting an arms fair) in Cardiff. He describes his experience in his witness statement, stating that the use of AFR made him feel "*uncomfortable*", "*alarmed*" and "*controlled*", and as though SWP was trying to "*intimidate [him] and other protestors*" at the arms fair [**SB/4/61; 63**]. He described the use of AFR at the protest as "*particularly distressing*", noting that he should have been able "*to protest peacefully … without my biometric data being captured*"; he described himself as concerned that his "*identity … [was] potentially being logged*" [**SB/4/63**]. He goes on to describe his view that where AFR is used at protests, "*people are encouraged to act differently in the knowledge that their identity may be traced and/or tracked*", and that people might not attend at all where AFR is deployed [**SB/4/62**]. Ms Irene, who was also present at the March 2018 deployment, felt she was "*[b]eing watched by AFR technology*" and stated that "*[t]he idea that my face could be being matched, and my identity known, is very scary"* [**SB/5/67**].

12. The December 2017 deployment took place during Christmas shopping; SWP's deployment report records its rationale as "*identifying and reducing the number of outstanding suspects*" in the area [**SB/14/139**]. The watchlist used contained over 900 people, including everyone sought on a warrant and every person wanted in connection with a crime in the police area. There were 10 matches (2 false positives and 8 true positives); two arrests were made (one person was arrested on suspicion of committing

offences under section 4 of the Public Order Act 1986 and criminal damage and the other for breaching the terms of a community order with a work requirement [**SB/8/97-98**] [**SB/14/140**]). The March 2018 deployment was rationalised on the basis that previous iterations of the arms fair had "*attracted disorder in both disruption to the event and wider community*", "*persons involved in previous protests against the arms fair had caused criminal damage and made a hoax bomb threat*" and a general aim to "*detain those wanted on warrant and local suspects*" [**SB/16/164**]. The watchlist contained approximately 500 people, including 6 who had previously been involved in disrupting the event and, in several cases, convicted of offences for the same. There was one true positive match but that was used purely for intelligence purposes and no steps were taken to arrest or speak to anyone [**SB/16/165**] [**SB/8/99-100**].

13. As set out above in Mr Bridges' and Ms Irene's statements, one of the key anxieties about AFR is that people do not know whether they are being monitored when engaged in lawful activities in public. In the course of the present litigation, SWP told the Appellant that he was not a person of interest to the police and had never been placed on a watchlist. There is no legal requirement on the police to provide such information, and it is inconceivable that the police would routinely, if ever, provide it outside of the present litigation. One of the uses of AFR is to determine if persons of interest for intelligence purposes are present at a particular location at a particular time. The usual policy of the police is, unsurprisingly, to neither confirm nor deny if someone is of intelligence interest. There is no indication that that policy is, or indeed ought to be, abandoned if AFR is to be rolled-out. The consequence is that, unlike the Appellant in the present case, individuals are very unlikely to be able to find out whether they are or are not included on AFR watchlists.

LEGAL FRAMEWORK

14. The legal framework applicable to SWP's use of AFR is set out in the Annex to the DC's judgment. SWP's use of AFR is based on a general common law power to obtain and store information for policing purposes. This is supplemented by the data protection principles contained in Part 3 of the DPA 2018. However, so far as the collection of personal data through AFR and the inclusion of persons on watchlists are concerned, it is only section 35 of the DPA 2018 (requiring lawful and fair processing) which is of relevance. In summary, this principle requires little more than that personal data processing is based on law and necessary for law enforcement purposes and a section 42 appropriate policy document (see

below) is in place. As such, it adds little to the requirements of Article 8(2) of the Convention (taken with section 6 of the HRA).

15. An additional component of the legal framework identified by the DC is the *Surveillance Camera Code of Practice* ("**the Code of Practice**"), to which SWP must have regard. It is promulgated by the Interested Party under the Protection of Freedoms Act 2012. This is not specific to AFR – indeed it predates police use of AFR – and has as its focus conventional CCTV. It includes one provision related to facial recognition which says no more than that its use must be justified and proportionate and that there should be human intervention before adverse decisions are taken. SWP published Standard Operating Procedures ("**the SoPs**") in November 2018 [**SB/23/237-261**]. These are therefore irrelevant to the December 2017 and March 2018 deployments but do form part of the current framework. They are essentially technical guidance aimed at operators of the system and focus on the practical aspects of AFR. The only relevant components concern the need for signage advertising deployments, a presumption that children should not be placed on watchlists and the desirability of AFR deployments being authorised by silver commanders.

16. The legal framework can, in essence, be distilled as a requirement that AFR use should be necessary for policing purposes and proportionate. Beyond these requirements, the police are essentially left to determine entirely for themselves how, when, and where to use AFR and who to include on watchlists and for what purposes. This legal framework is in stark contrast to those that apply to fingerprints and DNA, two other forms of biometric data commonly used by police. The taking of fingerprints and DNA and the further use of such data is underpinned by statute (primarily Part V of the Police and Criminal Evidence Act 1984) and the subject of detailed guidance (contained mainly in PACE Code D) setting out criteria for when and how the data can be taken and processed. This provides the "*detailed rules governing the scope and application of measures*" which Article 8 requires (*S v United Kingdom* (2009) 48 EHRR 50 at [99]).

C: GROUNDS OF APPEAL

GROUND 1: ARTICLE 8 – THE USE OF AFR IS NOT IN ACCORDANCE WITH THE LAW

17. The DC was, the Appellant respectfully submits, right to hold that the use of AFR engages the Article 8(1) rights of persons whose facial biometrics are captured, regardless of whether or not they are on a watchlist [**J/§62**]. The DC rejected SWP's argument that AFR

should be treated in the same way as the taking of a photograph by the police or merely observing someone in public. It held: "*AFR Locate goes much further than the simple taking of a photograph. The digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information*" [**J/§54**]. Applying S v United Kingdom, the DC held *"[l]ike fingerprints and DNA, AFR technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. Taken alone or together with other recorded metadata, AFR-derived biometric data is an important source of personal information … [this] is information of an "intrinsically private" character*" [**J/§57**]. However, the DC erred, it is submitted, in concluding that the interference with the Appellant's Article 8 rights occasioned by the use of AFR in December 2017, March 2018 and on an ongoing basis is in "accordance with the law" for the purposes of Article 8(2).

Legal principles

18. The principles governing the "in accordance with the law" requirement are broadly settled:

18.1. Measures or powers which interfere with rights under Article 8(1) must have a legal basis in domestic law. That basis must be "accessible" in the sense that it must be possible to discover, if necessary with the aid of professional advice, what its provisions are (e.g., Re Gallagher [2019] 2 WLR 509 at [16]-[17] per Lord Sumption).

18.2. The law must be *"sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*" (RE v UK (2016) 63 EHRR 2 at [122]). The law must be formulated with sufficient precision to enable any individual – if needs be with appropriate advice – to regulate his or her conduct (Sunday Times v UK (1979) 2 EHRR 245 at [49]).

18.3. The law must "*afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise*" (S v UK at [95]).

18.4. "*[S]afeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights*" (Beghal v Director of Public Prosecutions [2016] AC 88 at [32] per Lord

Hughes). Linked to this is the requirement that "*there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined*"; they "*should ensure that the national authorities have addressed the issue of the necessity…*" (*R (T) v Chief Constable of Greater Manchester Police* [2015] AC 49 at [114] per Lord Reed). The Supreme Court in *Christian Institute v Scottish Ministers* [2016] UKSC 61 considered a statutory provision permitting the sharing of information held about children which stated that information should not be shared unless it was "*necessary or expedient for the purposes of the exercise of [relevant] named persons functions*" (at [84]). The statutory power was accompanied by guidance reiterating the proportionality requirement and advising that records be kept of the rationale for sharing information. The Supreme Court held that the applicable legal regime did not enable "*proportionality to be adequately examined*" (at [84]) and that the regime was not therefore "*in accordance with the law*" (at [85]). It noted that "*[the relevant statute did] not address the factors to be considered in an assessment of proportionality and the [guidance] gives exiguous guidance on that issue*" (at [97]). It concluded *"[i]n order to reduce the risk of disproportionate interferences, there is a need for guidance to the information holder on the assessment of proportionality when considering whether information should be provided*" (at [101]).

19. Whether a measure is in accordance with the law is judged by reference to "*the potential reach of the power rather than its actual use*" because "*[a] power on which there are insufficient legal constraints does not become legal simply because those who may have resort to it, exercise self-restraint* (*Beghal* at [102] per Lord Kerr). *Beghal* concerned suspicionless port stops under the Terrorism Act 2000 and, although Lord Kerr dissented on the outcome of the appeal, his observation at [102] is orthodox. That is necessarily so because as Lord Sumption (with whom the majority agreed) held in *Gallagher*, whether or not a particular measure which interferes with qualified rights is in accordance with the law "*is not a question of degree*", it is *"[i]t is a binary test*". This assessment relates to the characteristics of the measure and not its application in any particular case (at [14]).

20. The European Court of Human Rights ("**ECtHR**") has consistently emphasised the importance of clear rules and safeguards governing the exercise of discretionary powers in the context of the state's use of surveillance and policing measures applying new (and

rapidly advancing) technologies (see e.g., *S v United Kingdom* at [103] and [112]). As far back as 1998 the ECtHR noted that *"[i]t is essential to have clear, detailed rules ... especially as the technology available for use is continually becoming more sophisticated*" (*Kopp v Switzerland* (1999) 27 EHRR 91 at [72]). More recently, in *Szabo & Vissy v Hungary* (2016) 63 EHRR 3, a case concerning covert surveillance, the ECtHR made the following observations about new technologies at [68]: [2]

> "*The techniques applied in ... monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*".

Submissions

21. SWP's use of live AFR is based upon a broad discretionary common law power which is not accompanied by documents with the quality of law required to satisfy Article 8(2). In particular the law does not: (i) indicate with sufficient clarity the scope of discretion conferred on SWP to use AFR; (ii) provide a sufficient indication of the circumstances in which and conditions on which AFR may be used and, in particular, when an individual may be placed on a watchlist and have their location and movements monitored and for what purpose; and (iii) provide safeguards which either have the effect of enabling the proportionality interference occasioned by the use of AFR to be adequately examined or guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interferences with Convention rights. As such, the DC erred in concluding that the legal framework generally provides a "*level of certainty and foreseeability that is sufficient to satisfy the tenets of Article 8(2)*" [**J/§96**] (see also [**J/§84**]).

22. First, the DC erred in concluding that there "*is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used*" [**J/§84**]:

    22.1. There is no guidance or policy (binding or otherwise) covering the circumstances in which and/or conditions on which a person is liable to be included on a police

[2] In *Catt v UK* (2019) 69 EHRR 7, the ECtHR held that these considerations apply equally to non-covert collection and retention of data (at [114]).

watchlist for use with AFR and for what purpose and/or when it would not be permissible to include a person on such a watchlist. Provided the inclusion is regarded as "necessary" for law enforcement purposes there is no limitation on who can be included or for what reason. Individuals can be included when suspected of no criminal offence, let alone a serious offence. They can be included purely for intelligence purposes. As set out above, there is no requirement that they be informed they are being monitored. For example, a person involved in a peaceful protest movement would not know whether (i) they could properly be included on an AFR watchlist for intelligence gathering purposes, with the result that their movements could be monitored or (ii) they are being monitored. Without any such criteria it is extremely difficult to foresee when one might and, more importantly would not, be monitored through AFR. Equally, this means that there is no meaningful constraint (other than technological limitations which, it may be inferred, shall quickly evaporate as the technology develops) on the number of people who could be included on a watchlist and whose location could be tracked around the country.

22.2. There is no guidance or policy on the locations at which AFR may be deployed. AFR use could, for example, be restricted in a code of practice or legal regime to named categories of venue, facility or event. Understanding where AFR is likely to be used and, therefore, being able to regulate one's behaviour accordingly is a key aspect of foreseeability. It is no answer to say that deployments are announced in advance and that signs are provided (people may not use social media or be in the habit of reading SWP's website and many people will not see or understand the significance of signs). As the DC stated [**J/§40**], many people are likely to be unaware that AFR is being used or how it is being used. Further, limiting the use of AFR to specific categories of location would ensure the proportionality of the use of AFR could be assured. It would ensure AFR could not simply be deployed on any street (and ultimately on all streets alongside CCTV).

23. Second, SWP's use of AFR cannot be said to be attended by safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. As set out above, the restrictions on the use of AFR amount to little more than stipulations that its use must be necessary and proportionate for law enforcement purposes. There is no guidance on how the proportionality of the proposed deployment of AFR is to be assessed.

Such guidance could make reference to the competing considerations which need to be considered. These considerations might, for example, include the seriousness of the offence for which particular persons suspected of being in the area are sought. Both the CJEU and ECtHR have held that the retention of and/or access to communications data can, for example, only be justified as necessary and proportionate for the purposes of preventing and detecting serious crime (*Tele2 Sverige AB v Post- och Telestyrelsen* (Joined Cases C-203/15 & C-698/15) [2017] QB 771 at [102], [119] and [125]; and *Big Brother Watch and others v United Kingdom* (2018) app nos. 58170/13, 62322/14 and 24960/15 [463] and [467]). Other constraints to ensure proportionality (and to enable proportionality to be examined in advance) might include restricting the use of AFR depending on (i) whether there are reasonable grounds for suspecting that persons on a watchlist will be present in the deployment area at the relevant time; (ii) the risk such persons are thought to pose to the public or particular places/events; (iii) the likely number of people whose facial biometrics will be captured during a given deployment; (iv) whether a large number of children are likely to be in the area; and (v) whether there are any known lawful protests which may be impacted by the deployment.

24. At present there are no measures which enable proportionality to be assessed. The case is therefore similar to *Christian Institute*: (i) as was the case in respect of some of the measures in issue in *Christian Institute*, SWP's use of AFR is an exercise of discretionary power, albeit one arising at common law rather than under statute, and (ii) as in *Christian Institute*, AFR is subject to the general provisions of data protection legislation. SWP's use of AFR therefore suffers from the same deficiencies as those considered in the *Christian Institute* case – there is no guidance on the assessment of proportionality.

25. Third, in holding that SWP's use of AFR was/is in accordance with the law, the DC relied in part on what it described as "*SWP's own policies*", namely (i) SWP's SoPs, (ii) SWP's deployment reports, and (iii) SWP's *Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 Data Protection Act 2018 (South Wales Police (SWP) Automated Facial Recognition (AFR))* ("**the Sensitive Processing Policy**") [**J/§§92-96**]. As the DC noted (at [**J/§80(1)&(2)**]), Article 8 requires that provisions must be "*published and comprehensible*" pursuant to the need for "*accessibility*". None of SWP's policy documents was in the public domain when SWP deployed AFR in December 2017 and March 2018. As such, they were not "accessible" and the Appellant respectfully contends that the DC

was wrong to rely on these documents in support of its conclusions that SWP's use of AFR on those occasions was in accordance with the law [**J/§§84; 92-96**]. Further, in respect of the ongoing use of AFR, neither the Sensitive Processing Policy nor SWP's deployment reports are made public. These documents were disclosed only for the purpose of this litigation. Furthermore, for the reasons explained under Ground 4 below, the DC cast considerable doubt on the lawfulness of the Sensitive Processing Policy [**J/§§139-141**].

26. Fourth, the DC erred in concluding that the data protection principles (alone or in combination with the other provisions identified) provide "*sufficient regulatory control to avoid arbitrary interferences with Article 8 rights*" (at [**J/§96**]). The data protection principles set out in Part 3 of the DPA 2018 (and, before that, Schedule 1 to the DPA 1998) offer little guidance or constraint in respect of the circumstances in which and conditions on which particular types of information may be collected. These broad principles are concerned principally with the retention and further use of personal data. Those provisions are too broad and general in nature to ensure that a technology, which allows the state to interfere with privacy rights of such a large number of people and to such an extent, operates in a manner that is non-arbitrary and proportionate. The first data protection principle, which is of primary relevance for the purposes of data collection, does little more than mirror the requirements of Article 8(2) that data processing is necessary and proportionate and for law enforcement purposes.

27. The DC's judgment in this regard places considerable weight on the majority's judgment in *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 in respect of the role of the data protection principles in fulfilling the "in accordance with the law" requirement [**J/§87**]. The appeals in *Catt* were, however, concerned with the retention of data. The appellants in *Catt* accepted that the collection of their data was lawful (at [1]) and the case said nothing about the circumstances in which individuals can be targeted for monitoring. In addition *Catt* was not concerned with surveillance involving the collection of the biometric data of thousands of people. In this respect, the use of AFR is more akin to publicly avowed bulk surveillance powers such as the retention of communications data and bulk interception where it is clear that the DPA alone does not suffice. In addition *Catt* was considered by the ECtHR (see *Catt v UK* (2019) 69 EHRR 7). While the ECtHR did not finally determine whether the inference with Article 8 rights occasioned by the retention of data on the "extremism database" at issue in the case was in accordance with the law (as

it found it to be disproportionate) it did make observations on the issue. It expressed "concern" about the "ambiguity" of this legal basis for retaining the material on the database (at [101]). In a concurring opinion, Judge Koskelo (joined by Judge Felici) stated that the legal basis was "*extremely vague and unspecific*" and continued: "*[t]he crucial importance of the quality of the law in a context such as the present one can be highlighted, most simply, by noting that that the general principles of data protection law—such as those requiring that the processing must be necessary for the purpose of the processing, … become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation*" (at [OI-6], see also [OI-9]).

28. Fifth, the Surveillance Camera Code of Practice and SWP's SoPs do not remedy the defects in the underlying legal framework. The Code of Practice contains a series of high-level principles (such as the need to have policies in place, see principle 5) and broadly repeats relevant data protection principles. The SoPs are concerned primarily with the practicalities of the operation of AFR. Both documents refer to the requirement for "proportionality" but tell decision makers next to nothing about how that is to be assessed.

GROUND 2: ARTICLE 8 – DISPROPORTIONALITY

29. The Supreme Court has set out the test for the assessment of the proportionality of the interference with a qualified right as follows: "*(i) whether the objective is sufficiently important to justify the limitation of a protected right, (ii) whether the measure is rationally connected to the objective, (iii) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and (iv) whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter (ie whether the impact of the rights infringement is disproportionate to the likely benefit of the impugned measure)*" (*Christian Institute* at [90]). It is submitted that the DC erred in its application of the fourth of these requirements for proportionality.

Submissions

30. It is clear from the above-cited test that when assessing whether an interference is proportionate it is necessary to consider the cumulative impact upon the rights of the persons (emphasis added) to whom it applies (i.e., not only the individual claimant before

the court). In the context of the deployment of AFR, this necessarily means considering, in the round, the Article 8 rights of *all* persons whose facial biometrics are captured during any given deployment. That is also clear from the Supreme Court's analysis in *R (Tigere) v Secretary of State for Business, Innovation and Skills* [2015] 1 WLR 3820. As the Court in *Tigere* made clear in analysing the fourth limb of the proportionality test, the court considers the benefits and impact on the community as a whole of a particular measure, not merely the impact on the individual claimant before the court (see discussion at [39]-[41] per Lady Hale).

31. It was common ground that thousands of people's faces are scanned during the course of each AFR deployment (SWP is able to count, but does not always do so, the total number of faces scanned during each deployment; see SWP's list of deployments [**SB/19/212-215**]). It was necessary, the Appellant submits, for the DC to consider the cumulative interference with the Article 8 rights of all those scanned on the two deployments at issue in determining proportionality. It did not do so. The DC considered only what it characterised as the "*very limited*" interference with the Appellant's Article 8 rights [**J/§101**]. It stated "*[t]he interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant's biometric data. No personal information relating to the Claimant would have been available to any police officer, or to any human agent. No data would be retained. There was no attempt to identify the Claimant. He was not spoken to by any police officer*" (emphasis added) [**J/§101**]. The Court did not attempt to quantify the total interference with Convention rights to which the two deployments at issue gave rise (i.e., how many people approximately had their biometric data extracted and analysed) and to weigh that against the reasonably anticipated benefits of the deployment. That is an error of law.

32. SWP has not disclosed the number of faces scanned during the December 2017 and March 2018 deployments (seemingly because it did not collect or retain this data). Data for the deployments at which this information has been provided indicate an average of 12,000 faces are scanned per deployment [**SB/19/212-215**]. The question the DC should have asked is whether, balancing the Article 8 and data protection rights of all those (approximately 12,000) individuals against the reasonably anticipated law enforcement benefits, the impact on their rights was proportionate.

33. Had the DC applied the correct test, the Appellant submits that SWP's use of AFR at the December 2017 and March 2018 deployments should have been found to be disproportionate. As to the reasonably anticipated law enforcement benefits, that should not be gauged by who was, in fact, apprehended as a result of the use of AFR on a particular occasion. Otherwise if no-one was apprehended (as is often the case) the use would inevitably be disproportionate. Instead, the DC should have examined the reasonably anticipated outcome of an AFR deployment by considering how many people are ordinarily located (there is an average of 2.35 positive alerts), and with what outcome (there is an average of 0.88 arrests per deployment), when AFR is used.[3] In respect of reasonably anticipated outcomes, the evidence demonstrates that arrests made on the basis of AFR have generally been for relatively minor offences [**SB/21/232-234**]. While the possibility of locating someone wanted in connection with a serious offence cannot be excluded, SWP's experience over a period of more than two years suggests that is very unlikely. In the Appellant's submission, the reasonably anticipated law enforcement benefits did not justify the inference with the Article 8 rights of an estimated 12,000 people for each deployment. Indeed, if such interferences are held to be proportionate, it is difficult to see why AFR could not be deployed across numerous public spaces on a regular or even permanent basis. If it is proportionate to capture and process the biometric data of 10,000 people on the basis that it is anticipated that one person will arrested for a relatively minor offence, it must be proportionate to capture and process the data of 1,000,000 people on the basis that it might lead to 100 such arrests.

GROUND 3: DPA 2018 – SWP'S DATA PROTECTION IMPACT ASSESSMENT

34. Pursuant to DPA 2018 section 64(1), data controllers are required to undertake a DPIA "*where a type of processing is likely to result in a high risk to the rights and freedoms of individuals*". A DPIA is an "*assessment of the impact of the envisaged processing operations on the protection of personal data*" (section 64(2)). This must be done prior to processing. Section 64(3) sets out the minimum requirements of a DPIA as: (a) a general

[3] These figures are based on SWP's table [**SB/19/212-215**] of deployment data from 66 deployments from 22 September 2017 to 28 September 2019 (the four Champions League deployments have not been included as it is accepted that these were deployments with significant problems, as is clear from statistics).

description of the envisaged processing operations; (b) an assessment of the risks to the rights and freedoms of data subjects; (c) the measures envisaged to address those risks; (d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Part 3 of the DPA 2018, taking into account the rights and legitimate interests of the data subjects and other persons concerned. Having in place a lawful DPIA is a condition precedent to lawful processing.

35. SWP undertook a privacy impact assessment in February 2018 [**SB/15/141-163**] and produced a DPIA in October 2018 (this remains the current version) in purported compliance with section 64 [**SB/17/166-206**]. The DC dismissed the Appellant's contention that SWP's DPIA did not comply with section 64 [**J/§148**]; the Appellant contends that it erred in doing so.

36. The DC held that the approach which should be taken by the court in respect of a challenge to compliance with the section 64 duty is akin to that taken in respect of the PSED [**J/§145**]. Noting that it is for the Court to decide whether the data controller has discharged that obligation, the DC said the following (with which the Appellant respectfully agrees):

> "***What is required is compliance itself, i.e. not simply an attempt to comply that falls within a range of reasonable conduct****. However, when determining whether the steps taken by the data controller meet the requirements of section 64, the Court will not necessarily substitute its own view for that of the data controller on all matters. The notion of an assessment brings with it a requirement to exercise reasonable judgement based on reasonable enquiry and consideration.* ***If it is apparent that a data controller has approached its task on a footing that is demonstrably false, or in a manner that is clearly lacking, then the conclusion should be that there has been a failure to meet section 64 obligation***" (emphasis added) [**J/§146**].

37. The DC held in respect of persons whose facial biometrics are captured but who are not on watchlists, that SWP's use of AFR both (i) engages their Article 8(1) rights, and (ii) constitutes the sensitive processing of their biometric data within the meaning of section 35 of the DPA 2018. SWP had contended throughout the litigation that Article 8 was not engaged in respect of such persons and that its use of AFR did not entail the processing of their (biometric) personal data. The Court rejected SWP's analysis of the law (see in particular [**J/§§52; 62 and 131–133**]). The DC, nevertheless, concluded that the DPIA "*recognise[d] that the personal data of members of the public*" (i.e., those not on a watchlist) was being processed [**J/§148**]. That is, it is respectfully submitted, wrong. SWP's incorrect understanding of the law is, unsurprisingly, reflected in its DPIA. The DPIA's

analysis of the application of data protection principles contains no recognition that AFR entails the processing of the personal data (and less still the biometric data) of persons not on watchlists. Nor does it acknowledge that the Article 8 rights of such persons are engaged. It is also silent as to the risks to other rights which are likely to be affected by the use of AFR: the rights to freedom of assembly and expression. SWP therefore approached its task of conducting a DPIA "*on a footing that is demonstrably false*" and/or "*in a manner that is clearly lacking*" [**J/§146**].

GROUND 4: DPA 2018 – SECTION 42 APPROPRIATE POLICY DOCUMENT

38. The DC concluded that SWP's use of AFR entails the sensitive processing of biometric data. As such, that processing had to comply with the requirements of section 35(3)–(5) of the DPA 2018. One of these requirements (see section 35(5)(c)) is for the data controller to have in place an "*appropriate policy document … in relation to the sensitive processing*" within the meaning of section 42(2) of the DPA 2018. The policy document must explain "*the controller's procedures for securing compliance with the data protection principles … in connection with sensitive processing"* (section 4(2)(a)) and "*the controller's policies as regards the retention and erasure of personal data processed"* (section 4(2)(b)). If no lawful section 42 policy document is in place, the "sensitive processing" of personal data will breach section 35 of the DPA 2018. The DC erred in failing to reach a conclusion on whether or not SWP had an "*appropriate policy*" in place [**J/§§139-141**].

39. The DC described SWP's Sensitive Processing Policy as being "*brief and lacking in detail*" and noted that it failed to "*address the position of members of the public*" (a reference to persons who are not on watchlists) [**J/§139**]. On this basis the Court stated, correctly the Appellant contends, that it is "*open to question whether this document … fully meets the standard required by section 42(2)*" [**J/§139**]. However, the DC declined to decide whether DPA 2018 section 35(5)(c) was satisfied, stating it would not be "*necessary or desirable for this Court to interfere*" [**J/§141**]. Instead, the Court confined itself to making the above "*observations*". This was not an option open to the DC.

40. First, compliance with DPA 2018 section 35(5) (taken with section 42(2)) is a condition precedent to lawful processing. Accordingly, the DC had to reach a conclusion on whether SWP's policy document complied with the DPA 2018 in order for it to conclude (as it did) that SWP's sensitive processing of biometric data complies with section 35. Second, as set

out above, the DC held that, on a complaint about a failure to comply with the obligation to undertake a DPIA under section 64 of the DPA 2018, the court is to decide for itself whether the data controller has discharged that obligation [**J/§146**]. In relation to the Sensitive Processing Policy, however, the DC declined to undertake that exercise. There is no warrant for treating the provisions differently. Both section 42(2) and section 64 impose conditions precedent for lawful processing. As with the DPIA, the DC was required to decide for itself whether the Sensitive Processing Policy satisfies section 42 of the DPA 2018.

41. Had the DC reached a conclusion it would have been bound to find that SWP's Sensitive Processing Policy did not comply with section 42(2). The document says almost nothing about the procedures for securing compliance with the data protection principles. Further, for the reasons given above in respect of the DPIA, SWP made a significant error of law in taking the view that its use of AFR does not entail the processing of the biometric data of persons not on watchlists. It is not therefore surprising that the Sensitive Processing Policy does not explain how SWP purports to secure compliance with the data protection principles in respect of such processing.

GROUND 5: PUBLIC SECTOR EQUALITY DUTY

42. The Appellant contends that the DC fell into error in holding that SWP complied with the PSED [**J/§§157-158**].

Legal principles

43. The principles applicable to the discharge of the PSED are uncontroversial and were summarised by McCombe LJ in *Bracking v Secretary of State for Work and Pensions* [2014] Eq LR 60 at [25]. So far as is relevant to this appeal, the applicable principles are: (i) "*A [decision maker] must assess the risk and extent of any adverse impact and the ways in which such risk may be eliminated before the adoption of a proposed policy and not merely as a 'rearguard action'*" (*Bracking* at [25(4)]; (ii) compliance with the PSED "*requires public authorities to be properly informed before taking a decision. If the relevant material is not available, there will be a duty to acquire it and this will frequently mean than some further consultation with appropriate groups is required*" (*R (Hurley & Moore) v SSBIS* [2012] HRLR 13 at [89] per Elias LJ; this is known as the duty of enquiry); and (iii) it is not sufficient simply to identify in general terms the potentially affected group, the

decision maker must "*fully appreciate the impact on those affected*" (*Bracking* at [40]) and *"be clear precisely what the equality implications are"* (*Hurley and Moore* at [78]).

44. What constitutes due regard is context dependent and "*will be influenced by a number of factors including, but not limited to, the nature of the decision being taken, the stage of the decision-making process that has been reached and the particular characteristics of the function being exercised*" (*R (Simone) v Chancellor of the Exchequer & anor* [2019] EWHC 2609 (Admin) at [63] per Lewis J). But the court has to be satisfied that "*there has been a rigorous consideration of the duty*" (*Hotak v Southwark LBC* [2016] AC 811 at [75] per Lord Neuberger PSC).

Submissions

45. The context in which SWP had (and has) to comply with the PSED, and the DC had to evaluate such compliance, is a trial of a new technology to be used in determining who the police should stop and question, where a problem of racial and gender bias has been identified as a "*feature*" common to the technology ([**J/§157**]). It is intended that the technology will be rolled-out to be used by police nationally where it will, no doubt, involve the scanning of thousands of faces on each deployment. The acute concerns that are raised, especially in relation to the risk of racial bias leading to erroneous police stops, are obvious. In that context, in order to comply with the PSED, SWP was required to make concerted efforts to determine whether the particular AFR software it was using suffered from the problems of race or gender bias identified in other software, and to take reasonable steps to obtain material to enable it to make that determination correctly. SWP failed to do so, and it is submitted that the DC erred in holding that SWP complied with the PSED.

46. The potential equalities implications of AFR have for a number of years (before SWP started using AFR) been widely reported in the media, by NGOs[4] and in the academic literature (cited in Dr Jain's First Expert Report [**SB/11/114-124**]). It is well established that "bias" is a common feature of AFR technology generally; this is on the basis of higher error rates in respect of (i) women and (ii) black people [**SB/12/127**]. As Dr Jain explains in his Second Expert Report, the risk that there will be significant differences in error rates is not marginal or trivial [**SB/12/127-128**]. One paper cited by Dr Jain, whose findings he

[4] See the examples cited at paragraph 89 of the Appellant's Statement of Facts and Grounds [**CB/15/239-240**].

concluded "*can be applied to AFR systems in general*", found the error rate for dark-skinned women to be more than 40 times higher than for lighter-skinned men [**SB/12/127**]. The reasons for the problems of bias are explained by Dr Jain. Essentially there is considerable evidence that the dataset with which AFR systems are "trained" has important implications for whether or not that system will have "biases" in relation to groups with particular protected characteristics [**SB/11/122-123**] [**SB/12/127-129**]. This is primarily due to the over or under representation of groups with particular protected characteristics in the training dataset. Further, as Dr Jain explains: *"if the demographic composition of the training dataset does not match the demographic composition of the population of the place where the system is deployed, then concerns of bias and discrimination arise*" [**SB/12/129**] (see also [**SB/11/123**]).

47. SWP relied on an Equality Impact Assessment ("**the EIA**") drafted in April 2017 [**SB/13/131-138**] (which was not updated in the 25 months between its being drafted and the hearing and, to the Appellant's knowledge, remains the only impact assessment relied on by SWP) to discharge its PSED. The EIA asked whether SWP's AFR system "*could have a differential impact*" (emphasis added) on grounds of race and sex [**SB/13/133-134**]. It concluded that it could not because "*AFR does not define race [or sex] of an individual*" [**SB/13/133-134**]. It therefore decided that no "*full impact assessment*" was required [**SB/13/138**]. That plainly does not discharge the PSED. Indeed it is based upon an obvious error of law. Consideration was given only to the possibility that AFR might be directly discriminatory, i.e., whether it could be used specifically to target those of a particular race or sex. No consideration was given to whether AFR might operate in an indirectly discriminatory manner, i.e., although applied equally to white and black people and to men and women, whether it might disadvantage those who were black or female because biases in the software meant it was significantly more likely to generate false positives in respect of those people. As such, SWP's conclusion that the AFR system it used "*could*" not have a "*differential impact*" based on race or gender was clearly not sustainable and does not come close to conducting the rigorous exercise required by the PSED in this context.

48. The DC, however, held that the EIA "*demonstrates … that due regard was had by SWP to the* [PSED]" [**J/§158**]. This, it is submitted, is an error of law. As set out above, the EIA gave no consideration at all to the potential that the AFR system it is using might suffer from the problem of race and gender bias that is a common feature of such systems, and,

instead, was premised on conflating direct and indirect discrimination, and concluding that because AFR is not being used to target people on the ground of race or gender it could not have a "differential impact".

49. The DC further held that "*[t]here is no suggestion that as at April 2017 when the AFR Locate trial commenced, SWP either recognised or ought to have recognised that the software it had licenced might operate in a way that was indirectly discriminatory. Indeed, even now there is no firm evidence that the software does produce results that suggest indirect discrimination*" [**J/§153**]. If the DC was concluding that there was no reason why SWP ought to have realised that any AFR software might operate in an indirectly discriminatory way, whether in April 2017 or subsequently, that is clearly inconsistent with the evidence (see above). If the DC considered that there was no requirement on SWP to conduct any assessment beyond the statement in its EIA that AFR could not have "a differential impact" on ground of race and gender because it did not have specific evidence of bias in relation to the software it was using provided by some third party, that is a misapplication of the PSED. The PSED (particularly in the acutely sensitive context raised in the present case) required SWP, for itself, to take reasonable steps to gather evidence on whether the software it was using might have the biases identified in many other AFR systems. It was not sufficient to state that others had not provided the evidence of bias.

50. The DC also considered evidence of PC Edgell (covering deployments between May 2017 and June 2018), the results of which are set out in a witness statement of 26 November 2018 [**SB/10/109-113**] (see [**J/§154]**). This analysis appears to have been undertaken in response to the current litigation, and long after AFR began to be used by SWP. Further, the analysis PC Edgell conducted was obviously flawed. He concluded that he has seen "*no bias based on either gender or ethnicity"* in the AFR system used by SWP [**SB/10/113**]. It is said that that conclusion is supported by correspondence between the ethnic demographic and gender breakdown of false positive results and true positive results. That is a flawed analysis and the data gathered by SWP is not capable of supporting PC Edgell's conclusion. In order to determine whether there is apparent bias in the AFR system, it would be necessary to compare the ethnic and gender breakdown of false positive alerts against the ethnic demographic and gender breakdown of *all faces scanned* by AFR (see the expert evidence of Dr Jain in response to PC Edgell's evidence [**SB/12/130**]). Yet, as PC Edgell

acknowledges in his statement, "*the identity of those who have passed the camera without generating an alert are unknown"* [**SB/10/111**].

51. The position, therefore, is that neither in April 2017 nor at the time of the hearing before the DC, did SWP have any way of knowing whether the technology it was using was likely to lead to a disproportionate number of black people and women being wrongly identified as of interest to the police. That remains the case. At no stage has SWP had access to, nor will it be able to obtain access, the dataset on which its system of AFR was/is "trained". That is because the supplier regards this information as a commercial secret and it does not appear that the SWP has required in its contract with the supplier to be able to access the information (including on a confidential basis). As Dr Jain explains, analysing the training dataset is necessary to determine if an AFR system is biased [**SB/11/123**] [**SB/12/127-129**]. Nor has SWP carried out any analysis which would examine the results of the AFR system it is using to see if they operate in a discriminatory manner (the analysis conducted by PC Edgell being flawed for the reasons set out above). That is not consistent with the PSED, it is submitted.

SOME OTHER COMPELLING REASON TO HEAR THE APPEAL

52. For the reasons set out above, the Appellant submits that his appeal has real prospects of success. Additionally or in the alternative, the Court is asked to grant permission to appeal on the basis that there are other compelling reasons why the appeal should be heard (CPR 52.6(1)(b)). The fact that a large number of people are affected by a measure, and the public interest in a particular issue, are good reasons for granting permission on this basis (see e.g., *Lloyd v Google LLC* [2019] EWCA Civ 1599 at [14]). As is apparent from the DC's judgment, this case raises issues of profound public importance and its determination necessarily affects large numbers of people – already, and in ever growing numbers should live AFR be rolled-out nationally. As the DC recognised, this is the first case to consider the legality of AFR. Its decision is likely to be taken as permitting AFR to be rolled-out nationally. If that occurs, it would constitute a sea change in the way communities are policed. It is not difficult to envisage AFR being deployed by police and other public authorities in many locations where CCTV is currently used.[5] The implications of this for

[5] By way of example, SWP has stated that CCTV systems currently operated could be equipped with AFR, and SWP recently announced that it is trialling using AFR on mobile phones – see

privacy and data protections rights are profound. There is therefore a strong public interest in the adequacy of the legal regime governing AFR being considered by the Court of Appeal.

D: CONCLUSION

53. For the reasons given above, the Appellant submits that permission to appeal should be granted on the five grounds set out above.

DAN SQUIRES QC
AIDAN WILLS
MATRIX

MEGAN GOULDING
LIBERTY

2 April 2020

https://www.south-wales.police.uk/en/newsroom/south-wales-police-trial-new-facial-recognition-app-on-officers-mobile-phones/ (accessed 25 October 2019).