CO/4085/2018

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT FOR WALES
BETWEEN:

THE QUEEN
(on the application of EDWARD BRIDGES)

Claimant

-and-

THE CHIEF CONSTABLE OF SOUTH WALES POLICE

Defendant

-and-

THE SECRETARY OF STATE FOR THE HOME DEPARTMENT

Interested Party

-and–

THE INFORMATION COMMISSIONER

-and–

THE SURVEILLANCE CAMERA COMMISSIONER

Interveners

SKELETON ARGUMENT ON BEHALF OF THE CLAIMANT

For the Substantive Hearing on 21 – 23 May 2019

References: Hearing Bundles [HB volume number/section letter/tab number/page]; witness statements and expert reports [surname /paragraph number]; Defendant's Detailed Grounds (D-DG § para); Secretary of State's Detailed Grounds (IP-DG § para).

Essential reading: Skeleton arguments; Statement of Facts & Grounds [HB1/A/2]; Defendant's and Interested Party's Detailed Grounds for Contesting the Claim [HB1/A/4-5]; Claimant's Reply [HB1/A/6]; Information Commissioner's Submissions [HB1/A/8]; Witness Statements of the Claimant [HB1/C/1] and of the Defendant [HB1/D/1-4]; Expert Reports of Dr Anil Jain [HB1/E/1-2]; Big Brother Watch Report [HB2/G/9]; Universities' Police Science Institute Evaluation of the Defendant's use of AFR [HB2/G/15]; Defendant's Draft Data Protection Impact Assessment [HB2/F/16] and Equality Impact Assessment [HB2/F/3].

A. INTRODUCTION AND OVERVIEW

1. This is the first case to consider the use of Automated Facial Recognition technology (**"AFR"**).[1] AFR involves the extraction of a person's biometric data from an image of their face and the comparison of this data with the facial biometric data from images contained in a database. The Defendant uses AFR to capture in real time and process the biometric data of up to 50 people per second for the purposes of locating persons of interest whose images are contained on so-called "watchlists" prepared for each deployment of AFR. The Defendant uses AFR in public spaces with significant footfall in order to maximise the chances of identifying such persons; he can capture and process the biometric data of tens of thousands of individuals on each occasion AFR is deployed. The overwhelming majority of persons whose biometrics are captured and processed by the Defendant using AFR are not suspected of any wrongdoing. The Defendant has been using AFR on a "trial" basis since May 2017 and has deployed it on approximately 40 occasions since then (up to April 2019). His trial of this technology is ongoing, with no specified end-date.

2. The collection of biometric data on an enormous scale represents a sea change in policing and seems set to continue given the rapid advances being made in AFR. The Claimant does not suggest that the Defendant or other police forces could never lawfully deploy AFR. He does, however, contend that its use has profound consequences for privacy and data protection rights and that the legal framework which currently applies to the use of AFR by the police does not ensure those rights are sufficiently protected. In that regard, AFR is not unique. There have been a series of instances in which the courts, and in particular the European Court of Human Rights ("**the Strasbourg Court**"), have found that relevant legal regimes have not kept pace with information-gathering technology.[2] To some extent that reflects the challenges new technologies inevitably pose for the law. It also, perhaps, reflects the tendency in the UK to adopt a less vigilant and more trusting approach towards state information gathering than has traditionally been shown in

[1] This is also known as Facial Recognition Technology (FRT), Automatic Facial Recognition Technology and Live Facial Recognition.

[2] Examples of this problem, all of which have led to the Strasbourg Court finding UK law wanting, include the targeted interception of communications and the obtaining of call logs (*Malone v United Kingdom* (1985) 7 EHRR 14 – leading to the adoption of the Interception of Communications Act 1985); the placing of listening devices in domestic premises (*Khan v United Kingdom* (2001) 31 EHRR 45 – which led to the amendment of the Police Act 1997); and the bulk interception of communications (*Liberty v United Kingdom* (2009) 48 EHRR 1 and *Big Brother Watch and others v United Kingdom* (2018) app nos. 58170/13, 62322/14 and 24960/15). See also *S v UK*, *Catt* and *Beghal* (for which the references are provided below) for other cases about information gathering powers.

continental Europe. As Lord Reed observed in *R (T) v Chief Constable of Greater Manchester* [2015] AC 49 at [88]:

> *The United Kingdom has never had a secret police or internal intelligence agency comparable to those that have existed in some other European countries, the East German Stasi being a well known example. There has however been growing concern in recent times about surveillance and the collection and use of personal data by the state. … But such concern on this side of the Channel might be said to have arisen later, and to be less acutely felt, than in many other European countries, where for reasons of history there has been a more vigilant attitude towards state surveillance. That concern and vigilance are reflected in the jurisprudence of the European Court of Human Rights in relation to the collection, storage and use by the state of personal data. The protection offered by the common law in this area has, by comparison, been of a limited nature*.

3. The Claimant contends that AFR is a further instance of the collection of personal data, and the level of surveillance that permits, which has been made possible by the development of a new technology being accompanied by insufficient legal constraints. In this regard, the fact that the use of AFR is currently being pioneered imposes particular responsibilities to ensure it operates within an appropriate framework that properly balances the law enforcement benefits of the technology with the implications for privacy and data protection rights. With considerable financial support from the Home Office, South Wales Police ("**SWP**") has become the national lead on the use of AFR in policing. As the Grand Chamber of the Strasbourg Court said in *S v United Kingdom* (2009) 48 EHRR 50:

> "*the protection afforded by art.8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests … any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard*" (at [112]).

4. These remarks were made 10 years ago in the context of a case concerning the gathering and retention of other forms of biometric data, namely DNA and fingerprints. They apply with equal force to AFR. The Claimant therefore welcomes the involvement of the

Divisional Court in shaping the legal parameters of the use of AFR in policing, in particular given that its use remains in a trial phase and before it is rolled-out nationally.

5. Lying at the heart of this case is a fundamental dispute about the understanding and categorisation of the privacy and data protection implications of the use of AFR. The Defendant's case is that his use of AFR does not even engage the privacy or data protection rights of the Claimant and, by extension, anyone whose facial biometrics are captured and processed through AFR but who are not included on a watchlist (D-DG § 43-44; 48; 69-70; 73; 75). The gravamen of the Defendant's argument is that such rights are not engaged because his use of AFR is akin to photographing or otherwise monitoring a person's activities in public and because, once taken and processed, his force does not retain the biometric data of those not on a watchlist. .

6. The Claimant contends that this analysis is wrong. It is based on an incorrect understanding of the privacy and data protection rights involved. The use of AFR involves the collection and further processing of the unique biometric data of large numbers of people. It is not analogous to the passive deployment of conventional CCTV by police. In terms of privacy and data protection rights, as deployed by the Defendant, AFR is analogous to taking the fingerprints or DNA (other forms of biometric data) of thousands of persons (if it could be done without their cooperation or consent), and comparing such biometric data to that of persons on a watchlist. Whether or not the DNA or fingerprints for non-matched individuals were then deleted, the obtaining and processing of the biometric data would plainly engage Article 8 of the European Convention on Human Rights ("**the Convention**") and data protection rights, and indeed would be a significant interference with those rights. It would, of course, not only be impractical but impermissible to take biometric data in that way (as it would breach one or more provisions in Part V of the Police and Criminal Evidence Act 1984 ("**PACE 1984**") and the accompanying statutory guidance). What is striking for present purposes, however, is that the taking of fingerprints and DNA biometric data and the further use of such data is underpinned by statute and the subject of detailed guidance setting out a series of criteria for when and how the data can be taken and processed. None of that applies to facial biometric data. There is no equivalent statutory basis or framework for the use of AFR by police. For the reasons set out below, the lack of a statutory basis and other legal constraints setting out with sufficient clarity the parameters of when and in what

circumstances facial biometric data can be taken and processed, means that the interference with privacy that it entails is not "*in accordance with the law*" for the purposes of Article 8 of the Convention.

7. In summary, it is the Claimant's case that, once the engagement of the relevant privacy and data processing rights of AFR is properly understood, it is apparent that the Defendant's use of AFR (on two occasions when the Claimant was present and on an ongoing basis) is:
    (a) incompatible with Article 8 of the Convention, primarily on the basis that it is not in accordance with the law but also because it was and is not necessary or proportionate (**Ground 1**);
    (b) that for similar reasons, it (i) breached the Data Protection Act 1998 ("**DPA 1998**") on the two occasions that – it is to be inferred – his personal data was processed (**Ground 3A**) and (ii) the Defendant's ongoing use of AFR is in breach of the Data Protection Act 2018 ("**DPA 2018**") (**Ground 3B**);
    (c) the Defendant failed to comply with his obligation to undertake a lawful Data Protection Impact Assessment ("**DPIA**") (**Ground 3C**); and
    (d) the Defendant failed to discharge the Public Sector Equality Duty ("**PSED**") in respect of his use of AFR (**Ground 4**).

B: FACTUAL BACKGROUND

AFR technology

8. AFR technology is explained in detail in the expert reports of Dr Anil Jain, a distinguished international expert in this field [HB1/E/1-2]. While Dr Jain does not comment directly on the specific AFR system/software used by the Defendant, he has expressed his confidence that his general comments on AFR systems apply equally to the Defendant's system (AJ2 § 10 [HB1/E/2/53]). AFR is comprised of the following steps:
    (1) Compiling/using an existing database of images. AFR requires a database of existing facial images (referred to in this case as "**a watchlist**") against which to compare facial images and the biometrics contained therein. In order for such images to be used for AFR, they are processed so that the "facial features" associated with their subjects are extracted and expressed as numerical values.
    (2) Facial image acquisition. A camera (which could be mounted on e.g., a van, lamppost or contained in a handheld device) captures individuals' facial

images. This may be done by (i) taking a static photograph in a "controlled" environment (for example where an individual has her photograph taken at a border gate when presenting a passport); or (ii) capturing a moving image when a person passes into the camera's field of view, using a live feed. This case is concerned with the latter, i.e., the use of AFR cameras in real time, in a "live" context.

(3) Face detection. Once an AFR camera used in a live context captures footage, the software (i) detects human faces and then (ii) isolates individual faces.

(4) Feature extraction. Taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face.

(5) Face comparison. The AFR software compares the extracted facial features with those contained in the facial images held on pre-existing databases.

(6) Matching. When facial features from two images are compared, the AFR software generates a "**similarity score**". This is a numerical value indicating the likelihood that the faces match, with a higher number indicating a greater likelihood of a positive match between the two faces. Operators of AFR systems are generally able to amend the "**threshold [of similarity] value**", above which a similarity score is taken to indicate a potential match. As Dr Jain explains (AJ1 § 34) [HB1/E/1/6-7], fixing this value too low or too high can, respectively, create risks of a high "**false alarm rate**" (i.e., the percentage of incorrect matches identified by the software) or a high "**false reject rate**" (i.e., the percentage of true matches that are not in fact matched by the software).

(7) Action taken on the basis of a potential match.

9. AFR is therefore a powerful form of technology which has the potential to identify (negatively or positively) a very large number of people in real time. Depending on the size and scope of the watchlist used, it is theoretically possible to identify (with some measure of certainty) everyone within a crowd of people without interacting with them or seeking their consent.

The nature of the data processed through the use of AFR

10. The use of AFR technology involves the collection, processing and storage of a range of information including facial images, facial features (which are biometric data), metadata

(including time and location) associated with the same and information as to matches with persons on a watchlist.

11. AFR entails the processing of *biometric data* in the form of facial biometrics. "Biometrics" are defined in the Interested Party's Biometrics Strategy (2018) [ ] as "*the recognition of people based on measurement and analysis of their biological characteristics or behavioural data*" (§ 1) [HB2/G/11/128]. The DPA 2018 defines biometric data as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data*" (section 205(1) of the DPA 2018). The unique identification of individuals on the basis of / in association with biometric data is important because it is this that distinguishes biometrics from other forms of data. The exploitation of biometric data enables the state to determine with considerable accuracy where an individual has been and, potentially, what they may have been doing.

12. Alongside fingerprints and DNA, facial biometrics are one of the primary forms of biometric data (as is reflected in the Biometric Strategy [HB2/G11/131-135]). Facial biometrics are most closely analogous to fingerprints because (a) both can be captured without the need for any form of intimate sampling and (b) both concern a part of the body that is generally visible to the public (see e.g., C-291/12 *Schwarz v Stadt Bochum* [2014] 2 CMLR 5 at [48]). Facial biometrics are potentially of greater utility, and a more powerful tool, than fingerprints because, through AFR, they are far easier to obtain and can be procured without requiring the cooperation of the subject or the use of force. Indeed, through AFR the facial biometrics of vast numbers of people can be obtained without their being aware.

The use of AFR by the Defendant

13. The Defendant is the national lead on AFR and has received substantial grants from the Interested Party for these purposes. AFR has been used by SWP since May 2017 and continues to be used on an ongoing basis (see the list of deployments appended to the Chronology and provided at [HB2/F/19]).

14. The Defendant uses two forms of AFR: AFR Locate and AFR Identify (see the description at [HB2/E/15/177-180]). This case concerns only the former and all references to AFR

should be read as such. As the name suggests, the purpose of AFR Locate is to "locate" people "within a crowded environment"; this is done in "live time" or real time (Lloyd § 6, 8 [HB1/D/2/8-9]; Draft Data Protection Impact Assessment [HB2/F/16/204]). The Defendant uses AFR for locating "persons of interest", which term is not defined but appears to include persons ranging from those who are wanted on warrants, to those suspected of having committed crimes and persons who are simply of possible interest to SWP for intelligence purposes (Lloyd § 24 [HB1/D/2/8-9]; Universities' Police Science Institute Evaluation – "UPSI Report" [HB2/G/15/177]).

15. Watchlists containing "candidate images" of persons of interest are created for each deployment of AFR; several colour-coded watchlists may be used for a single deployment (Lloyd § 17, 23 [HB1/D/2/10-11]; UPSI Report [HB2/G/15/177]). These appear to be compiled primarily (but not exclusively) from images held on SWP's Niche Record Management System – a database of custody photographs (Methven § 6 [HB1/D/3/27]; Lloyd § 16, 22 [HB1/D/2/10-11]). But there does not appear to be any limitations as to the source of the images used.[3] Images are "enrolled" into the AFR system, meaning that a biometric template is taken from the images – this is used for the purposes of undertaking algorithmic comparisons with the facial biometrics of persons captured on camera.

16. SWP uses video cameras, which have hitherto been mounted on stationary police vans or on poles/posts, for capturing "probe images" of the face of anyone who passes within range of the camera. The AFR software isolates facial images from the live footage, extracts the facial biometrics of each subject and processes this data to ascertain whether the facial biometrics match those of a person on the watchlist being used for the deployment. It appears that the Defendant's system is now set to detect up to five faces in a given frame (DG-DG § 7) and may capture 10 frames per second. Where there is a potential match, a system operator assesses the two images and an intervention may then be made.

17. The Defendant stated "*intention during each deployment [is] to allow the AFR application to enrol and therefore process* ***as many individuals as possible***" (emphasis added) [HB2/F/16/218]. While the Defendant does not routinely record the total number of

[3] In the Defendant's Draft Data Protection Impact Assessment it is stated that "*[w]atchlists will wherever possible be born from custody images*" [HB2/F/16/219].

people whose facial biometrics are captured and processed as part of each deployment of AFR, it is clear that these numbers are vast. By way of example, it is estimated that approximately 21,500 were scanned in the context of a Rugby Union international in November 2017, and approximately 44,500 during the course of a weekend event in Swansea [HB2/F/5/66; HB2/F/15/200].

18. Although the Defendant does not appear to have used AFR covertly, it can reasonably be inferred that the vast majority of persons whose facial biometrics are processed in the context of the Defendant's use of AFR are not aware that this has happened. Indeed it is the Claimant's evidence that he did not see signage and was given no other warning indicating that AFR was in use prior to his being in close proximity to AFR-equipped vans (Bridges § 9, 15-16) [HB1/C/1/2-4].

Use of AFR on 21 December 2017

19. An AFR equipped van was deployed on Queen's Street between 8AM and 4PM and the system was live for the entire deployment (Lloyd § 49 [HB1/D/2/19]; Operational Deployment Debrief [HB2/F/8]). The Defendant avers that AFR was deployed in Cardiff City Centre "*with a focus on locating and detaining*" wanted offenders (Lloyd § 47 [HB1/D/2/17]). The evidence on the composition of the watchlists for this deployment suggests that AFR was deployed to locate a single person suspected of having committed a serious crime, a large number of people (382) "*wanted on warrant*" and an even larger group (a further 536) "*suspected of committing criminal offences*" (a further 536) with the effect that "*every single person*" suspected of committing a crime in the Defendant's police area was included on a watchlist (Lloyd § 52 [HB1/D/2/19-20]; Operational Deployment Debrief [HB2/F/8]). The watchlist used included more than 900 persons.

20. As he relays in his witness statement, the Claimant was present on Queen Street, Cardiff, on 21 December 2017 when an AFR-equipped van was deployed (Bridges § 7-10) [HB1/C/1/2-3]. He was as close as approximately 6-10 feet from the van and was accordingly in range of the cameras (Bridges § 10) [HB1/C/1/3].

Use of AFR on 27 March 2018

21. AFR was deployed at the Defence, Procurement, Research, Technology and Exportability Fayre ("**the Arms Fair**") held at the Motorpoint Arena in Cardiff on 27 March 2018. AFR

was deployed – and was live – between 8:30AM and 4PM with the cameras focussing on the arena's entrance (Lloyd § 61 [HB1/D/2/22]).

22. According to the Defendant, AFR was deployed on the basis that previous iterations of the event "*had attracted disorder*" and that persons involved in past protests had caused criminal damage and made two bomb hoax calls to disrupt the event (Lloyd § 60 [HB1/D/2/21]; Operational Deployment Debrief [HB2/F/11]). On this footing, AFR was used to locate 6 persons arrested at previous iterations of the Arms Fair, most of whom had been convicted of a variety of offences. It is unclear why these persons were being sought and, in particular, it is not suggested that they were suspected of having committed further offences for which they were being sought. Indeed it is Inspector Lloyd's evidence that one of these individuals was sought so that a police officer could engage in "*dialogue*" with them to "*ensure their behaviour was of an appropriate nature*" (Lloyd § 64(a) [HB1/D/2/22]). AFR was also deployed for the purposes of locating 347 persons wanted on warrants and a further 161 people for reasons that are not clear[4] (Lloyd § 64(b) [HB1/D/2/22-23]; Operational Deployment Debrief [HB2/F/11]). In respect of this cohort of more than 500 persons, there is no suggestion that their actions which gave rise to a warrant being issued for their arrest had any connection with the Arms Fair. No arrests were made in respect of this deployment (Operational Deployment Debrief [HB2/F/11]).

23. The Claimant attended a protest outside the Arms Fair. He was within range of the AFR-equipped van. Prior to seeing the van (and, it is to be inferred, being scanned by its cameras) the Claimant was not aware that AFR was in use and he did not observe the Defendant's officers providing any information about its use (Bridges § 11 -16 [HB1/C/1/3-4]).

C: LEGAL FRAMEWORK

24. There is no statutory power authorising the use of AFR in the context with which this case is concerned. For the reasons developed below, the Defendant has wrongly suggested that the statutory basis for his use of AFR is to be found in section 35 of the DPA 2018 (D-DG § 35-36; 55). He has not provided any further explanation as to the legal basis for his use

[4] The rationale for the Purple Watchlist, which is referred to in the Operational Deployment Debrief, is not covered in Inspector Lloyd's evidence.

of AFR on a continuing basis. Nor has the Defendant explained the legal basis upon which he relies in respect of his use of AFR on 21 December 2017 and 27 March 2018, prior to the entry into force of the DPA 2018. The Interested Party avers that the Defendant – and, presumably, the police generally – may undertake AFR on the basis of their common law powers (IP-DG § 15; 17).

Protection of Freedoms Act

25. Chapter I of Part 2 of the Protection of Freedoms Act 2012 ("**PFA**") makes limited provision for the "*regulation of CCTV and other surveillance camera technology*". The PFA does the following:

    (1) Defines a "*surveillance camera system*" as including: "*(a) closed circuit television or automatic number plate recognition systems, (b) any other systems for recording or viewing visual images for surveillance purposes, (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b) …*" (section 29(6)).

    (2) Section 29(1) mandates the Secretary of State (the Interested Party) to prepare a code of practice containing guidance about surveillance camera systems. That code was issued and published under sections 30 and 32 of the PFA in June 2013 as the *Surveillance Camera Code of Practice* (see below) ("**the Code of Practice**").

    (3) Section 33 requires "*relevant authorities*" (which includes a chief officer of a police force) to have regard to the Code of Practice when exercising any functions to which it relates.

    (4) Section 34 creates the statutory post of Surveillance Camera Commissioner ("**SCC**") and lays down a mandate for the SCC, which includes (a) encouraging compliance with the Code of Practice, (b) reviewing the operation of the Code, and (c) providing advice about the Code (including changes to it or breaches of it).

Surveillance Camera Code of Practice

26. The focus of the Code of Practice is 12 guiding principles concerning the operation of surveillance camera systems. These include the following:

    2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. …

    5. Clear rules, policies and procedures must be in place before a surveillance camera system is

used, and these must be communicated to all who need to comply with them. …

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

27. Most of the Code of Practice concerns "conventional" CCTV systems but the following is said in reference to AFR: "*[a]ny use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely*" (§ 3.2.3).

SCC guidance on police use of AFR

28. The SCC has published non-statutory "guidance" or "advice" (both terms are used) entitled *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems* ("**SCC AFR Guidance"**). This is designed to assist relevant authorities in complying with their statutory obligations "*arising under section 31(1)*" of the PFA and the Code of Practice (§ 1.3).[5] The SCC AFR Guidance is promulgated on the basis that the SCC "*should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems*" (Code of Practice § 5.6). It is said that the SCC AFR Guidance indicates "*the way in which the Commissioner is minded to construe the particular statutory provisions arising from PoFA* [PFA] *and those provisions within the SC Code* [the Code of Practice] *in the absence of case law*" (§ 1.8).

29. The SCC AFR Guidance focuses on the assessment of the necessity and proportionality of deployments of AFR. It also provides advice on conducting risk assessments and making use of the SCC's 'Self-Assessment Tool'. In respect of watchlists there are suggestions concerning the nature of images used to produce watchlists.

30. Unlike the Code of Practice, there is no requirement for the Defendant to have regard to the SCC AFR Guidance. This Guidance was first published in October 2018 and re-published without changes in March 2019. It therefore has no relevance to the Claimant's

[5] It is assumed that this reference is intended to be to section 33 because section 31(1) concerns the Secretary of State keeping the Code of Practice under review.

Article 8 and DPA 1998 claims in respect of the Defendant's use of AFR on 21 December 2017 and 27 March 2018. In any event, as non-binding advice, the SCC AFR Guidance does not constitute "law" for the purpose of Article 8(2) of the Convention.

Data protection legislation

31. Two data protection regimes are relevant to this claim. The Claimant's data protection claims in respect of the Defendant's processing of the Claimant's personal data through his use of AFR on 21 December 2017 and 27 March 2018 fall to be determined under the DPA 1998. His challenge in respect of the Defendant's ongoing use of AFR is governed by the DPA 2018.

DPA 1998

32. Section 1(1) of the DPA 1998 defined personal data as "*data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*". Data processing was defined in the same section as "*obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data*" (with a range of non-exhaustive examples given).

33. Section 4(4) made it "*the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller*" (subject to section 27(1) concerning the exemptions – the Defendant has not indicated that he relies on any such exemption). The data protection principles were set out in Schedule 1 to the Act. The only principle relevant for the purposes of this claim was contained in paragraph 1 of that Schedule; it provided that "*[p]ersonal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met…*" Schedule 2 included the following conditions (in so far as is conceivably relevant):

> *1. The data subject has given his consent to the processing.*
>
> *5. The processing is necessary –*
>
> *(a) for the administration of justice,*
>
> *(b) for the exercise of any functions conferred on any person by or under any enactment,*
>
> *(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or*
>
> *(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.*

34. The DPA 1998 did not contain any definition of biometric data; nor was such data included within the definition of sensitive personal data within section 2 of the Act.

DPA 2018

35. Contrary to what is suggested by the Defendant (see D-DG § 23-27; 37), the data protection provisions applicable to his use of AFR (from 25 May 2018) are to be found in the DPA 2018 (and Part 3 in particular) and *not* in the General Data Protection Regulation ("**GDPR**"). Nor is Part 3 of the DPA 2018 the domestic legislation contemplated by Article 9 of the GDPR (cf. D-DG § 27). Part 3 of the DPA 2018 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the EU Law Enforcement Directive 2016/680 ("**the Law Enforcement Directive"**). Article 2(2)(d) of the GDPR specifically provides that the Regulation does not apply to data processing "*by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*". Part 3 of the DPA 2018 applies to "*the processing by a competent authority* [which the Defendant is, pursuant to section 30(1) and Schedule 7 to the Act] *of personal data wholly or partly by automated means*", provided that such processing is for law enforcement purposes (which definition is included in section 31 and mirrors the abovementioned definition in Article 2(2)(d) of the GDPR).

36. Section 3(2) defines "personal data" as "*any information relating to an identified or identifiable living individual*", *which means an individual "who can be identified, directly or indirectly, in particular by reference to – (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual*". Biometric data is defined in section 205(1) in the terms set out above (see paragraph 11).

37. Part 3 of the DPA 2018 contains a number of data protection principles the only one of which that is relevant for this claim is section 35, the material parts of which provide that:

> *(1)The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.*
>
> *(2)The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that* ***it is based on law*** *and either –*
>
> *(a)the data subject has given consent to the processing for that purpose, or*

(b)the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3)In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4)The first case is where –

(a)the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where –

(a)the processing is strictly necessary for the law enforcement purpose,

(b)the processing meets at least one of the conditions in Schedule 8, and

(c)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(8) In this section, "sensitive processing" means –

(b)the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual (emphasis added).

38. Section 42 contains requirements in respect of the "appropriate policy document" referred to in section 35(4), including the stipulation that:

(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which –

(a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period –

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, […]

39. Among the conditions referred to in Schedule 8 (referenced at section 35(5)) is:

Statutory etc purposes

This condition is met if the processing –

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

40. The Defendant is incorrect in his assertion that section 35 provides a legal basis for AFR. That data processing must have some independent legal basis is plain from the requirement in section 35(2) that the processing must be "based on law" and the narrative contained in the Explanatory Notes.[6] If the position were otherwise, there would be no need for any statutory (or other legal basis) for, by way of example, the taking of fingerprints or even the interception of communications.

Standard operating procedures

41. The Defendant has in place standard operating procedures ("**SOPs**") which apply to his use of AFR [HB2/F/26]. This document is not public and its provisions are not legally binding. As such the SOPs *do not* form part of the applicable legal framework and the Defendant is correct not to rely upon them (D-DG § 23-32).

D: GROUNDS

GROUND 1: ARTICLE 8

42. Article 8 of the Convention provides that:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

ENGAGEMENT OF ARTICLE 8

43. The test for the engagement of Article 8(1) in the context of informational privacy is whether a person has "*a reasonable expectation of privacy*" (or "*a reasonable expectation of protection*")[7] in respect of particular information (or, more specifically, a reasonable expectation that such information will not be used by the defendant in a particular way) (see e.g., *Re JR 38* [2016] AC 1131 at [87] – [88] per Lord Toulson and [105] per Lord Clarke).

[6] Paragraph 184 stipulates that "*"Lawful" processing means authorised by either statute, common law or royal prerogative. For example, Part 5 of the Police and Criminal Evidence Act 1984 (which applies to England and Wales) confers statutory authority for the taking and retention of DNA and fingerprints…*".

[7] Following the Supreme Court's decision in *JR 38* the Claimant accepts that this court is bound to accept that this is the relevant test for engaging Article 8. He notes, however, that since this decision the Grand Chamber of the ECtHR has held that the engagement of Article 8 in cases concerning the use of information may not be limited to circumstances in which there is a reasonable expectation of privacy (*Barbulescu v Romania* (2017) 44 BHRC at [73]). The Claimant's position on this is expressly reserved.

This "*must extend to every occasion on which a person has a reasonable expectation that there will be no interference with the broader right of personal autonomy recognised in the case law of the Strasbourg court*" (*R (Catt) v Association of Chief Police Officers* [2015] AC 1065 at [4] per Lord Sumption).

44. Whether or not a person has a reasonable expectation of privacy in respect of particular information requires an assessment of all of the circumstances of the case and "*on the underlying value or collection of values which article 8 is designed to protect*" (*JR 38* at [97] per Lord Toulson). *JR 38* involved a challenge to the police releasing images to local newspapers of those engaged in sectarian rioting and violent offending. Because the conduct of the person in question is relevant to whether there exists a reasonable expectation of privacy, it is easy to understand why the Supreme Court in *JR 38* did not consider Article 8 to be engaged in respect of a person engaging in a riot because "*the criminal nature of what the appellant was doing was not an aspect of his private life that he was entitled to keep private*" (*JR 38* at [112] per Lord Clarke). The same was true in relation to the police noting down a person's movements as part of an investigation into criminal activity; "*[t]he criminal nature of what he was doing, if that was what it was found to be, was not an aspect of his private life that he was entitled to keep private*" (*Kinloch v HM Advocate* [2013] 2 AC 93 at [21] per Lord Hope).

45. The Claimant's primary position is that Article 8 is engaged on the basis that he had (and has) a reasonable expectation that his facial biometrics (a unique identifier) would not be taken and processed by SWP, without his consent, in circumstances in which he was engaged in lawful activities in a public place and was not suspected of any wrongdoing. It matters not that the Claimant was not on a watchlist (when AFR was deployed on 21 December 2017 and 27 March 2018) and may not be placed on a watchlist in future. This contention is founded on the following propositions.

46. First, for the reasons developed below under Grounds 3A and 3B, it is the Claimant's position (with which the Information Commissioner agrees) that AFR involves the processing of personal data and also amounts to the "sensitive processing" of biometric data of persons whose faces are scanned, regardless of whether or not they are on a watchlist. While it is not always the case that the processing of personal data will engage Article 8, the symbiotic relationship between privacy and data protection rights is well

established. The Grand Chamber of the Strasbourg Court has emphasised the significance of the protection of personal data as part of Article 8. In S v UK (2009) 48 EHRR 50 the Court stated that "*[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by art.8 of the Convention* (at [103] – see also Satakunnan Markkinaporssi Oy v Finland (2018) 66 EHRR 8 at [137]).

47. For its part, the Court of Justice of the European Union ("**the CJEU**") has repeatedly emphasised that the right to protection of personal data is "*closely connected with the right to respect for private life*", and that "*the right to respect for private life with regard to the processing of personal data*" is founded on both Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("**the Charter**") and extends to "*any information relating to an identified or identifiable individual*" (C-468/10 and C-469/10 ASNEF v Administración del Estado [2012] 1 CMLR 48 at [41] – [42]; see also C-291/12 Schwarz v Stadt Bochum [2014] 2 CMLR 5 at [26]).

48. Second, biometric data is recognised as being a particularly sensitive form of personal data. Both the EU (Article 9 of the GDPR and Article 10 of the Law Enforcement Directive) and UK legislatures (sections 10 and 35 of the DPA 2018) have given special protection to biometric data through data protection legislation. This is plainly of relevance to the question of whether Article 8 is engaged.

49. Third, both the Strasbourg Court and the CJEU have emphasised the importance of biometric data as part of the right to privacy. S v UK was a case concerning the retention of DNA samples and fingerprints of persons who had not been convicted. The Grand Chamber accepted that the retention of both categories of biometric data amounted to an interference with Article 8 (at [77] and [86]). The Court considered such data to be of an "*intrinsically private*" character (at [104]). It is the Claimant's case that this reasoning applies with equal force to facial biometrics. While the case concerned the long-term retention of biometric data, there is nothing in the Grand Chamber's decision to suggest that Article 8 is not engaged through the initial obtaining of such data. Indeed, logically, the characterisation of information (as falling with the ambit of Article 8) cannot depend on the particular use being made of it or for how long it is retained. In the context of the interception of communications, the Strasbourg Court has treated the interception (i.e., the

initial gathering of the information in question), the retention of that information and any subsequent use of the information as discrete interferences with Article 8 (see for example *Amann v Switzerland* (2000) 30 EHRR 843 [GC] at [48] and [69]). This rationale, the Claimant submits, also applies to the gathering and retention of biometric data.

50. In *Schwarz*, a case concerning a person's refusal to provide his fingerprints in the context of obtaining a passport, the CJEU noted that fingerprints "*objectively contain unique information about individuals which allows those individuals to be identified with precision*" (at [27]). It held that both the taking and retention of fingerprints "*constitutes a threat to the rights to respect for private life*" (at [30]). The Court went on to accept that the taking of fingerprints and facial images engaged Articles 7 and 8 of the Charter (at [49]).

51. The reason that the taking and processing of biometric data engages privacy rights is that such data is a highly personal and unique identifier, capable of identifying an individual with precision. Taken together with the metadata recorded by, for example, AFR systems, facial biometric profiles, like biometric data derived from DNA and fingerprints, are a powerful source of sensitive information for law enforcement agencies. It is this sensitivity, and capacity for identification with precision, which calls for regulation of the collection of such information. The Defendant contends that facial biometric profiles are unlike other forms of biometric information because they are "*manifest in public*" (D-DG § 50). This is misconceived. While facial biometric profiles are generated on the basis of a person's facial features (which undoubtedly may be manifest in public), the precision of biometric identifiers (which are expressed as a numerical code and are not visible to humans) and the extent to which they are unique to the individuals processed, are far beyond that which is perceptible by members of the public or a police officer reviewing a CCTV feed. Fingerprints are derived from the unique whorls and ridges on a person's fingertips which are observable by anybody looking at that person's hands. However, it cannot sensibly be suggested that this renders a fingerprint any less sensitive as a unique and precise identifier of an individual.

52. Fourth, one of the primary regulators in this field, the SCC, has issued guidance which is strongly supportive of the proposition that AFR engages Article 8 rights. The SCC AFR Guidance notes that Article 8 is a "*fundamental consideration*" in the context of the "*overt operation of surveillance camera systems*"; the SCC goes on to state that the "*use of AFR … in*

crowded places and selected sites will significantly enhance the capabilities of a surveillance camera system to intrude and gather private information of a citizen" (§ 2.1 – 2.2). The SCC refers to the "*intrusive capabilities of AFR*" (§ 9.2) and expresses the view that "*potential for intrusion arising from AFR is arguably consistent with that arising from some forms of covert surveillance tactics and capabilities*" (§ 10.2). It is plain that this remark is not confined to persons whose images are contained on watchlists.

53. Further, in the context of this litigation the Information Commissioner has stated that: "*the automated capture of facial biometrics, and conversion of those images into biometric data, involves large scale and relatively indiscriminate processing of personal data. If such processing is not subject to appropriate safeguards, such data … could be collected … in a manner amounting to a serious interference with privacy rights*" (IC § 18). Such statements from the regulators with responsibility in this area lend further support to the submission that the capturing and processing of facial biometrics by police through AFR engages Article 8.

54. Fifth, the Claimant is of good character and there is no suggestion that on either 21 December 2017 or 27 March 2018 he was engaged in any reprehensible or criminal conduct. That is an important consideration in relation to whether an individual has a reasonable expectation of privacy in relation to photographs or observations of their movements in public (see *JR 38* and *Kinloch*). It is still more important where one is concerned not with the mere taking of photographs but the capturing of biometric data. He and others are entitled to expect that, if they conduct themselves lawfully in public, their biometric data will not be taken without their consent and, that if the police do wish to take their biometric data, they do so pursuant to lawful authority and only where necessary within the meaning of Article 8(2).

55. Sixth, the Strasbourg Court has on a number of occasions held that the taking of photographs or CCTV footage engages Article 8. In *Reklos v Greece* [2009] EMLR 16 the Strasbourg Court set out the general principle that "*[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*" (at [40]). The Court continued "*[t]he 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*" and it held that that control included the right to object to the recording of a person's image without their consent (ibid). In the

recent case of *Antovic & Mirkovic v Montenegro* (2017) application no. 70838/13, the Strasbourg Court accepted that Article 8 is engaged by the use of overt CCTV in lecture theatres at a public university (at [45]).

56. The domestic courts have suggested that the "*bare act*" of taking photographs by the police of a person not engaged in any unlawful activity in a public place will not engage Article 8 in the absence of "*aggravating circumstances*" (see the obiter dicta of Laws LJ in *R (Wood) v Commissioner of Police for the Metropolis* [2010] 1 WLR 123 at [36] & [39]). In *Wood* the taking of photographs of a campaigner leaving an arms fair was found to engage Article 8, and the "*aggravating circumstances*" included that the Claimant did not know why his photograph was being taken and what use might be made of it (see [43] and [45]-[46]). The present case plainly does not involve the "*bare act*" of taking a photograph. It involves the use of video cameras connected to sophisticated technology which extracts and analyses facial biometrics. Furthermore, as in *Wood*, all that the Claimant knew was that he was being surveilled by AFR cameras which would extract biometric data (although a vast majority of those passing the cameras would not even know this) but he did not know why SWP was doing so and what use may be made of his data.

57. For the reasons set out above, it is submitted that Article 8 was engaged on the two occasions when the Claimant's facial biometrics were captured and further processed, and would be engaged if he was subject to the technology again in the future. That is irrespective of the fact that he was not on a watchlist on either of the two occasions and he may not be on a watchlist in the future.

THE DEFENDANT'S USE OF AFR IS NOT IN ACCORDANCE WITH THE LAW

Legal principles

58. In order for an interference with Article 8(1) to be "in accordance with the law" for the purposes of Article 8(2), the following requirements must be satisfied.
    (1) The measure in question must have some basis in domestic law.
    (2) It must be "compatible with the rule of law" which means that it should comply with the twin requirements of "accessibility" and "foreseeability".
    (3) The legal basis must be "accessible" to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are.

(4) The measure must also be "foreseeable" meaning that it must be possible for a person to foresee its consequences for them and it should not "*confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself*" (Re Gallagher [2019] 2 WLR 509 at [17]).

(5) Related to this is the need for the law to "*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]). Where, as in this case, the impugned measure is a discretionary power what is required is that "*safeguards 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).

(see further Lord Sumption's overview of the case law in Re Gallagher at [16] – [31] and the cases cited therein).

59. In S v UK the Grand Chamber held that for the purposes of the retention and use of fingerprints and DNA (i.e., two other forms of biometric data) it was necessary for there to be, among other safeguards, "*detailed rules governing the scope and application of measures*" in order for the interference with Article 8 rights to be in accordance with the law (at [99]). The Court went on to state that: "[*t*]*he domestic law must afford appropriate safeguards to prevent any … use of personal data as may be inconsistent with the guarantees of [Article 8].* ***The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes***" (at [103] – emphasis added).

60. It is trite that when assessing whether a particular power is in accordance with the law, it is not necessary to demonstrate that the measure in question was exercised arbitrarily in respect of a specific instance in which it was used. As Lord Kerr observed in Beghal (dissenting, albeit not in respect of this uncontroversial proposition):

> "*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. It is the potential reach of the power rather than its actual use by which its legality must be judged*" (at [102]).

Submissions

The common law is an insufficient legal basis for collecting biometric data

61. The Defendant has not been clear on the legal basis for his use of AFR. His *Policy on Sensitive Processing for Law Enforcement Processing* (November 2018) makes the vague assertion that "*the lawfulness of South Wales Police processing is derived from its official functions as a UK police service*" [HB2/F/17/243]. The Defendant's Detailed Grounds suggest that section 35 of the DPA 2018 is the legal basis for his use of AFR; for the reasons set out at paragraph 40 above, this analysis is incorrect. The only possible legal basis is the common law.

62. On the assumption that the Defendant relies on the common law as the "law" on the basis of which he uses AFR, it is submitted that the common law is not sufficient to underpin the large-scale processing (without consent) of biometric data. This is because AFR is qualitatively different from the police taking photographs (which can be done pursuant to common law powers, see *Wood* at [54] and [98]) and the type of data collection and retention with which the Supreme Court was concerned in *R (Catt) v Association of Chief Police Officers* [2015] AC 1065 (at [1] and [7]). *Catt* was a case concerning the retention in the so-called National Extremism Database of a photograph of the claimant and, inter alia, brief information as to his attendance at protests, his address and date of birth. In *Catt* Lord Sumption (with whom the majority of the Court agreed) held that: "*at common law the police have the power to obtain and store information for policing purposes … These powers do not authorise intrusive methods of obtaining information…*" (at [7]). He held that the common law was a sufficient legal basis for the police to create the Extremism Database.[8]

63. It is the Claimant's case that the use of AFR to obtain biometric data without a subject's consent (and in many cases without their knowledge) may properly be regarded as "intrusive" in the sense used by Lord Sumption. As such, the common law provides an insufficient legal foundation for its use – there is a need for a statutory basis, as is the case for the taking of fingerprints and DNA samples. For the reasons set out above, there is a

[8] Mr Catt failed in his case before the Supreme Court but was recently successful in Strasbourg, where the Court held that the retention of the information in question amounted to a disproportionate interference with his Article 8 rights (*Catt v United Kingdom* (2019) ECHR application no. 43514/15). The Strasbourg Court expressed concerns about the legal basis for the database (see esp [105]) but ultimately left open the question of whether it was "in accordance with the law". The Claimant accepts that *Catt* in the Supreme Court remains binding but as set out above is readily distinguishable from the present case.

particularly strong analogy between the collection of facial biometrics and biometric fingerprint data. Indeed it is arguable that the interference occasioned by the taking of facial biometric data is significantly greater than fingerprint data. This is because facial biometrics can be used to compile a record of an individual's movements and/or to surveil them in real time in a way that fingerprints cannot. Yet the contrast in terms of the legal basis for the taking of fingerprints as compared to facial biometrics is stark. Section 61(1) of PACE 1984 lays down the general principle that fingerprints cannot be taken without a person's consent other than as is provided for by that section. PACE 1984 and PACE Code D (Code of Practice for the identification of persons by Police Officers ["**PACE Code D**"] a statutory code of practice issued under section 66 of PACE 1984) lays down detailed conditions on the taking and further processing of fingerprint data. The Claimant submits that similar statutory protection is required for the taking and processing of facial biometrics through AFR.[9]

Insufficient safeguards and/or a lack of foreseeability

64. Even if the common law is regarded as providing a sufficient legal basis for the Defendant's use of AFR, the interference with the Claimant's Article 8 rights is not in accordance with the law owing to a lack foreseeability and insufficient safeguards to circumscribe the Defendant's discretion to use AFR and to prevent the arbitrary use of this form of biometric information gathering. In assessing the adequacy of safeguards, it is submitted that is necessary to have regard to the fact that, in any single deployment, the use of AFR engages the Article 8 rights of many thousands of people.

65. The police's common law powers to obtain and retain information for policing purposes confer an extremely broad discretion to collect information, including through the use of AFR. It is limited only by public law principles and the requirements that the gathering of information is necessary in pursuit of some proper policing purpose. In his concurring opinion in *Catt v United Kingdom* Judge Koskelo characterised this common law legal basis as being "*about as vague as it can get*" (Concurring Opinion at [7]). Regardless of whether

[9] It is recognised that the taking of fingerprints generally requires the cooperation of, or use of force on, the subject while the taking of facial biometrics does not. That does not alter the privacy analysis. If technology was developed so that the police were able to take fingerprints, or indeed DNA, without the knowledge or consent of an individual, that would breach Article 8(2) unless there was some statutory basis. General common law powers would not suffice. Indeed the fact that biometrics can be taken without a person's knowledge or consent makes the requirement for a clear legal basis all the more important.

or not common law powers are a sufficient legal basis for AFR, Article 8 requires robust legal provisions to circumscribe the exercise of a discretion to use AFR to gather biometric data and to provide sufficient safeguards to prevent arbitrary and/or disproportionate use of AFR.

66. The existing legal framework is inadequate in this regard. In particular:

(1) There is no explanation – less still any circumscription – as to the circumstances in which and the specific policing purposes for which, AFR may be deployed. On the basis of what the Defendant has said during the course of this litigation, it appears that AFR may be used to "*identify and apprehend*" offenders (D-DG § 1) and to "*locate persons of interest*" (Edgell § 2 [HB1/D/4/33]). The latter include "*vulnerable persons and other persons where intelligence is required*" [HB2/F/16/230].[10] Yet there is no legal framework / criteria governing whether/when AFR may be used for the purposes of *inter alia* locating persons: (i) suspected of committing offences for which they have not yet been apprehended; (ii) who are unlawfully at large having failed to surrender to custody or for whom there is a warrant out for their arrest; (iii) who are suspected – on reasonable grounds (or otherwise) – of being about to commit a specific offence at an event/place at which AFR is deployed; or simply (iv) persons whose presence in a particular place SWP wishes to be aware of (indeed there appears to be no restriction on using AFR for "intelligence gathering" purposes, for example to determine who is present at a demonstration or other public gathering). The lack of prescribed purposes for obtaining facial biometrics is in stark contrast to the position in respect of the taking of fingerprints.

(2) There is no requirement that the deployment of AFR be limited to locating persons who are reasonably suspected of posing a threat to the event, location or persons frequenting a particular place (as opposed to persons who are wanted on suspicion of having committed offences generally). The consequence of this is that the Defendant deploys AFR in places/at events primarily on the basis that it is known that there will be a high footfall and that the prospect of locating a person of interest may therefore be increased.

[10] There is no definition of the terms "offender" or "person of interest" in any document relied on by the Defendant.

(3) Linked to (2) is the absence of limits on the seriousness of (suspected) offences or offenders whose potential presence at a given event or place may justify the use of AFR. Notably, there is no requirement that AFR may only be deployed for the purposes of locating persons who are suspected of having committed or being about to commit a serious crime or indictable offence. Nor is there any requirement that the use of AFR be limited to locating those who have committed criminal offences or are reasonably suspected of having done so. Such limitations are likely to be a significant safeguard against the arbitrary/disproportionate interference with Article 8 rights of persons whose facial biometrics are captured.

(4) Equally, there are no published criteria for the inclusion of a person's image on a watchlist. This is particularly important in circumstances in which it is not difficult to imagine SWP (and other forces) using even larger and untargeted watchlists derived from images held on the Police National Database or those held on the kind of database considered in *Catt* of those who have attended particular demonstrations. Technological or contractual restrictions[11] alone are plainly an insufficient constraint in this regard.

(5) Nowhere in law are there limits as to the permissible sources of images included on watchlists. While the Defendant avers that he has not used images derived from social media (D-DG § 12(1)),[12] there is no published guidance on whether this (or the use of images from other, non-police database sources) would be permissible and, if so, in what circumstances.

(6) There is no provision as to the locations / types of location at which the Defendant may deploy AFR.

(7) There is no indication as to whether individuals must be warned that their biometric data is being taken and processed or any restriction on AFR being used covertly.

(8) While the Defendant has averred that the biometric data captured through AFR is immediately deleted and the facial images against which alerts are made are in any event deleted within 24 hours (see Lloyd § 46 [HB1/D/2/16]),

[11] See the SOPs [HB2/F/26/283].

[12] The Claimant notes that this appears to be disputed by the authors of the Universities' Police Science Institute's *Evaluation of South Wales Police's use of Automated Facial Recognition Technology*, [HB2/G/15/183].].

that is a matter of practice and practicality. No such rules are set out in any publicly available, legally binding document; and, consequently, SWP could retain and process such data for longer.

(9) There is no requirement that the Defendant monitor the total number of persons whose facial biometrics are captured (it has been stated on behalf of the Defendant that SWP simply seeks to do this "where possible" – Edgell § 9-11 [HB1/D/4/34]). The absence of any such requirement is significant because this data is central to the assessment of the proportionality of the use of AFR (see by analogy see e.g. *Iordachi v Moldova* (2012) 54 EHRR 5 at [51] and *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at [84]).

67. The absence of conditions, constraints and safeguards on the collection and further processing of facial biometrics through the use of AFR compares unfavourably with the position in respect of biometric fingerprint data. Pursuant to PACE 1984 specific conditions must be satisfied before fingerprints can be taken, including where a person has been detained in consequence of his being arrested for, charged with or convicted of "*a recordable offence*", or a person is reasonably suspected of committing or attempting to commit an offence and their name is not known/cannot be ascertained. PACE Code D sets out further requirements including the need to inform the person concerned of: the reason their fingerprints are to be taken; the power under which they are to be taken; the fact that their fingerprints may be the subject of a speculative search against other fingerprints; and the fact that their fingerprints may be retained in accordance with particular provisions (§ 4.7). PACE 1984 also regulates the subsequent use of fingerprint data and contains very detailed provisions on the retention and destruction of such information (sections 63D to 63Q in particular). There are no equivalent statutory (or statutory guidance) provisions governing the collection of facial biometrics and no bespoke provisions regulating the retention and subsequent use of such information.

68. The Defendant places considerable reliance on the DPA 2018. While it is accepted that Part 3 of that Act is a relevant (and necessary) component of the legal framework governing the use of AFR, it is not sufficient to render the taking and further processing of facial biometric data "in accordance with the law". Part 3 of the DPA 2018 – and the data protection principles contained therein – is necessarily generic. The data protection principles focus primarily on data retention and the further use of retained data (for

example the purpose limitation [section 36], accuracy and keeping data up to date [section 38] and keeping data for no longer than is necessary [section 39]). While these provisions are relevant to data obtained through AFR, the data protection principles contain little of specific relevance to determine when and in what circumstances the capturing of facial biometrics through AFR is or is not permissible. The following observation of Judge Koskelo in his concurring opinion in *Catt v United Kingdom* is apposite: "*the general principles of data protection law – such as those requiring that the processing must be necessary for the purpose of the processing, and that the data to be processed must be adequate, relevant and not excessive in relation to that purpose – become diluted, possibly to the extent of practical irrelevance, where the purpose itself is left without any meaningful definition or limitation*" (Concurring Opinion at [6]). This issue arises in the context of AFR because the purposes for which it may be used are not defined or limited; this diminishes the protective effect of the data protection principles in the DPA 2018 (and indeed in the DPA 1998).

69. Both the Defendant and the Interested Party rely on safeguards provided by section 35(5) of the DPA 2018 (D-DG § 27-28, 38-40; IP-DG § 6, 8-9). The Defendant's primary position, however, is that section 35 does not apply to the use of AFR in relation to persons who are not on a watchlist in respect of the deployment in question. If that is correct it has no relevance for the purpose of Article 8(2) in a case such as the Claimant's. As set out below (paragraphs 87-88), the Claimant submits that that is an incorrect interpretation of section 35(8). However, the fact that section 35 defines the processing of biometric data as "sensitive processing" does not, in itself, render use of AFR "in accordance with the law." In essence it means, as with any other "sensitive processing", that the processing must be "strictly necessary" for law enforcement purposes and that the police must have a policy document in place pursuant to section 42 of the DPA 2018. That does not provide the safeguards required by Article 8(2) any more than it would in other contexts where processing of private information takes place. For example, interception of communications will in many cases involve "sensitive processing" as defined by section 35(8) of the DPA 2018. It could not seriously be suggested that the DPA 2018, of itself, therefore provides a sufficient legal basis for interception. Nor would the DPA 2018 be sufficient in relation to the taking and processing of DNA and fingerprints simply because that too is "sensitive processing". The question will, in every case, be whether, taken overall, there are sufficient legal constraints in place given the nature of the interference

at issue. For the reasons set out above, the Claimant submits there are not in relation to AFR.

70. Furthermore, and without prejudice to the Claimant's position that section 35 (and indeed Part 3 of the DPA 2018 generally) does not provide sufficient safeguards to ensure that inferences occasioned by the use of AFR are in accordance with the law, the reliance placed on this provision serves to underline the manifest lack of safeguards in place in December 2017 and March 2018 when the Claimant's facial biometrics were captured and processed. Indeed at these times, the legal framework for the Defendant's use of AFR was essentially limited to the common law, the DPA 1998 and Article 8 taken with section 6 of the Human Rights Act 1998 ("**HRA**"). This was insufficient to ensure that interferences with the Claimant's Article 8 rights were in accordance with the law.

71. The Code of Practice and/or the SCC AFR Guidance are not sufficient to remedy these defects. The Code of Practice contains broad principles of general application which do not answer the need for foreseeability and appropriate safeguards in the legal framework for AFR. The SCC AFR Guidance focuses primarily on the process of assessing necessity and proportionality – reciting principles of general application that are well established. Moreover, police forces are not required to have regard to the SCC AFR Guidance – it has the status of non-statutory "advice". It cannot constitute "law" for the purpose of Article 8(2).

NECESSITY AND PROPORTIONALITY

Legal principles

72. In order for an interference with Article 8 rights to be "necessary in a democratic society" it must correspond to a pressing social need and be proportionate to the legitimate aim pursued. The test applicable to the assessment of the proportionality of a measure was set out in *Bank Mellat v Her Majesty's Treasury (No 2)* [2014] AC 700 (at [20] per Lord Sumption and at [74] per Lord Reid) and includes the following elements:
    (1) whether the objective the measure pursued is sufficiently important to justify the limitation of a fundamental right;
    (2) whether it is rationally connected to the objective;
    (3) whether a less intrusive measure could have been used; and

(4) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

Submissions

73. It is, of course, accepted that law enforcement is a sufficiently important aim so as, in principle, to justify the limitation of an individual's privacy rights. The Claimant also accepts that the Defendant's use of AFR has been rationally connected to that aim. It is submitted that the interferences with the Claimant's Article 8 rights when (it can be inferred for the reasons set out at paragraphs 19-23 and 77) his facial biometrics were taken and processed on 21 December 2017 and 27 March 2018 were, nevertheless, disproportionate for the following reasons, which focus on the third and fourth limbs of the test in *Bank Mellat*:

    (1) At each deployment, the Defendant's use of AFR interfered with the Article 8 rights of thousands of people, not suspected of any wrongdoing. This is plainly relevant to the question of whether, assessed in the round, a fair balance has been struck between the rights of these individuals and the interests of the community.

    (2) The Defendant deployed AFR on 21 December 2017 and 27 March 2018 not for the purpose of locating persons who were assessed (on reasonable grounds) to pose a specific threat to the event or location in question but to take advantage of the presence of large numbers of people to have the potential opportunity to locate a person of interest. As concerns 21 December 2017, the Claimant's private information (and that of many thousands of others) was processed for the purposes of identifying and reducing the number of suspects in the area [HB2/F/8]. The use of AFR on 27 March 2018 was for the "*purposes of monitoring the area*" and seeking to detain "*those wanted on warrant and local suspects*" [HB2/F/8]. The Defendant therefore used a measure that interfered with the Article 8 rights of the Claimant and many others in a wholly untargeted and, it may be said, speculative manner. Moreover, at the 27 March 2018 deployment, one of the persons was being sought simply to enable the police to engage in dialogue with them for the purposes of giving them a warning as to their conduct (Lloyd § 64 [HB1/D/2/22]). Further, it is apparent that the AFR was deployed in part to "monitor" the area because SWP

considered there to be limited conventional CCTV coverage. This suggests that, had such systems – which are less intrusive of Article 8 rights – been available, it may have been unnecessary to use AFR [HB2/F/11]. In these circumstances, the balance between the Claimant's rights and the interests of the community was not fairly struck.

(3) At both deployments, AFR appears to have been used in the hope of locating persons wanted in connection with summary only offences – the use of AFR was not limited to those who were being sought in respect of serious crime or indictable offences.[13] Attempting to locate persons suspected of having committed summary only offences was not, the Claimant submits, a sufficiently weighty reason to justify the interference with his Article 8 rights and those of thousands of others.

74. As to the Defendant's ongoing use of AFR, the starting point is that the Defendant bears the burden of justifying as necessary and proportionate for specified law enforcement purposes the interference with the Article 8 rights of the very large numbers of innocent people (who are not on watchlists) whose biometric data is taken and processed through the use of AFR. While the Defendant does not routinely monitor the figures, it may reasonably be assumed that, at every deployment of AFR, the Defendant has interfered with the Article 8 rights of thousands (and in most cases in excess of ten thousand) people. To date, the Defendant's use of AFR has probably resulted in the taking and processing of biometric data of hundreds of thousands of people. As it is currently operated, his use of AFR generally suffers from essentially the vices identified in relation to the deployments on 21 December 2017 and 27 March 2018 at paragraph 73 above. For the following reasons, the Defendant's ongoing use of AFR does not strike a fair balance between the rights of the hundreds of thousands of people who have their biometrics taken and processed and the interests of the community in enabling SWP to pursue law enforcement purposes:

(1) The Defendant's use of AFR is untargeted and speculative. He is deliberately using AFR in places in which there are large numbers of people for the

[13] See by way of analogy the stipulations in the Investigatory Powers Act 2016 (e.g., sections 20(2) and 106(1)) that powers can only be used for the purposes of "preventing or detecting serious crime", which is defined in section 263 as an offence for which a person who has reached the age of 18 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more. Following the CJEU's lead, the Strasbourg Court held in *Big Brother Watch & ors v UK* that it was a violation of Article 8 to permit access to communications data for the purposes of combatting "crime" as opposed to "serious crime" (at [467] – [468]).

purposes of capturing the facial biometrics of as many people as possible in the hope that he may locate one or more persons of interest. AFR is being used to seek persons who are not assessed to pose any risk to the place or event in question.

(2) AFR is being used for locating people who are not suspected of having committed (or being about to commit) criminal offences. There is no requirement – or practice – that AFR only be deployed for such purposes and, less still, any requirement that AFR be used – and the Article 8 rights of many thousands of innocent persons be interfered with – only when a person or persons are suspected of committing serious criminal offences and/or posing immediate risks.

(3) The Defendant has not established that there are not less intrusive means available to SWP for pursuing the legitimate law enforcement aims for which AFR is deployed. Specifically, he has not shown that there are no other appropriate means available by which he could locate persons of interest that do not involve taking and processing the biometric data of hundreds of thousands of persons who are not suspected of any wrongdoing. These means include those used by police forces which do not use AFR (the Claimant is not aware of any evidence that such forces have greater difficulties than SWP in locating persons who are, e.g., suspected of committing offences) as well as those used by SWP before it acquired AFR and still used in addition to AFR. The Defendant has not adduced evidence to suggest that there has been a relevant change to SWP's capacity to locate criminals since he started using AFR so as to justify the scale of the interference with Article 8 rights. Plainly, the mere fact that a technology is available (and may lead to some savings in terms of resources) cannot mean that its use can be justified as proportionate.

GROUND 3A: BREACH OF THE DATA PROTECTION ACT 1998

75. It is the Claimant's case that his personal data was processed unlawfully by the Defendant in the context of SWP's use of AFR on (i) 21 December 2017 and (ii) 27 March 2018. This processing caused him distress. As such, the Defendant is wrong to characterise this aspect of his claim as being of "historic interest" (D-DG § 68).

The Claimant's facial biometrics were captured

76. The Defendant says that it "*is not (and cannot now be) known*" whether the Claimant's facial biometrics were captured on either relevant occasion (D-DG § 17). He contends that there is "*no evidence that the Claimant's image was recorded*" but accepts that "*it is impossible to know*" and in relation to the 27 March deployment "*it cannot be ruled out*" (D-DG § 19 and 22).

77. On the basis of the following facts, the Claimant invites the Court to draw the inference that his facial biometrics were captured and processed on each occasion:

    (1) The Claimant's evidence is that on 21 December 2017 he was approximately 6 to 10 feet from an AFR-equipped van (Bridges § 10 [HB1/C/1/3]). He took a photograph of the van, which is exhibited to his statement and provided at [HB2/G/3]; this illustrates his close proximity to the side of the van. He has looked at the map of the deployment location contained in Operational Deployment Debrief and confirms that he was within the applicable "orange box" (Bridges § 10 [HB1/C/1/3]).

    (2) On 27 March 2018 the Claimant attended the Arms Fair protest at lunchtime at which point he saw an AFR-equipped van; he walked along the pavement in front of the arena and was within the "orange box" shown on the Defendant's Operational Deployment Debrief and he was at one point fewer than 25-30 metres from the van (Bridges § 12-14 [HB1/C/1/3]).

    (3) The Operational Deployment Debrief for Arms Fair deployment states that the 2 cameras were facing the entrance to the Arena [HB2/F/11].

    (4) It is Inspector Lloyd's evidence that the AFR system was live between 8AM and 4PM on 21 March and between 8:30AM and 4PM in respect of the Arms Fair deployment (Lloyd § 49 and 61 [HB1/D/2/19 & 22]).

    (5) The AFR cameras have a range of up to 75 metres [HB2/F/26/285]. The Defendant's AFR cameras were capable of capturing between 50 and 300 faces per second [HB2/G/15/182].

The Claimant's personal data was processed through the Defendant's use of AFR

78. Assuming that the Court draws the inference that the Claimant's facial biometrics were captured on one or both of the abovementioned occasions, it is submitted that this plainly amounted to the processing of his personal data of which the Defendant was the data

controller. The Claimant's image and facial biometrics are his personal data within the meaning of section 1(1) of the DPA 1998 because he can be identified from those data.[14] The Claimant respectfully adopts the Information Commissioner's submission that "*facial images collected by AFR are 'personal data'*" (IC § 13). While this statement was made in respect of the definition of personal data contained in section 3 of the DPA 2018, it applies equally to personal data under the DPA 1998. Further, in C-212/13 *Rynes* [2015] 1 WLR 2607 (at [21] – [25]), the CJEU accepted that the image of a person captured by CCTV surveillance of a public space (by a private individual) constituted their personal data provided that the person can be identified (directly or indirectly).

The Claimant's personal data was processed unlawfully

79. The Defendant's processing of the Claimant's personal data was in breach of section 4(4) of the DPA 1998 on the basis that it did not comply with the first data protection principle. First, it was not lawful because it was in breach of Article 8 of the Convention for the reasons set out under Ground 1. If the Claimant is correct about this, the processing of his data was necessarily in breach of the first data protection principle.

80. Second, the processing did not meet any of the conditions in Schedule 2 to the DPA 1998. Two of the Schedule 2 conditions on which the Defendant seeks to rely (D-DG § 72) are not relevant: processing necessary for the compliance with a legal obligation [paragraph 3] (the Defendant has not identified any such obligation); and processing necessary for the administration of justice [paragraph 5(a)] (processing in the context of AFR is not concerned with the administration of justice, as is indicated by the Information Commissioner in respect of the DPA 2018 [IC § 24]). Whether or not he can rely on the other conditions he cites (processing necessary for the exercise of functions conferred by or under any enactment [paragraph 5(b)]; processing necessary for the exercise of any other functions of a public nature exercised in the public interest [paragraph 5(d)]; and processing necessary for the purposes of legitimate interests pursued by the data controller [paragraph 6]) comes down to an assessment of necessity/proportionality of the data processing in question.

[14] Support for this analysis is found in the Article 29 Working Party's *Opinion 02/2012 on facial recognition in online and mobile services*, in which it is stated that "*[w]hen a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data*" (p.4).

81. In the context of the Schedule 2 conditions, necessity "*means more than desirable but less than indispensable or absolutely necessary*" and, while a data controller has some margin of appreciation in determining what is necessary when relying on Schedule 2 conditions, it must act proportionately (*R (Hussain) v Sandwell Metropolitan Borough Council* [2018] PTSR 142 at [230] per Green J).

82. The Defendant's processing of the Claimant's personal data was not necessary and proportionate for the reasons set out in paragraph 73 above.

83. The Claimant suffered distress by reason of the Defendant's breach of the first data protection principle, as he describes in his witness statement (Bridges § 30-32 [HB1/C/1/6]). The Defendant does not dispute the Claimant's evidence in respect of distress in either his Detailed Grounds or the evidence filed by him.

GROUND 3B: SECTION 35 OF THE DATA PROTECTION ACT 2018

84. The Defendant's continuing use of AFR is in breach of section 35 of the DPA 2018.

85. For substantially the same reasons given in respect of the DPA 1998 (see paragraph 78 above), the Defendant's capturing and further processing of facial biometrics through AFR constitutes the processing of personal data (of which he is the data controller) within the meaning of section 3 of the DPA 2018. The Information Commissioner has expressed her agreement with this analysis (IC § 13-14). The use of AFR includes other discrete acts of data processing with which this ground of challenge is not concerned (including the compilation of watchlists and the storing or any further use of data gathered through or for the purposes of AFR).

86. The Defendant is a "competent authority" within the meaning of section 30 of the DPA 2018 (taken with Schedule 7 to that Act) and his data processing in the context of the use of AFR constitutes processing for law enforcement purposes as defined in section 31 of the DPA 2018. As such, pursuant to section 29 of the DPA 2018, Part 3 of the DPA 2018 applies to the Defendant's processing of personal data in respect of all aspects of AFR. Processing for law enforcement purposes must comply with the data protection principles contained in sections 35 to 40 of the DPA 2018.

87. The first data protection principle (contained in section 35 of the DPA 2018) requires that processing be lawful and fair. Since the use of AFR entails the processing of biometric data, it amounts to "sensitive processing" within the meaning of section 35(8), which includes "*the processing of … biometric data, for the purpose of uniquely identifying an individual*". The Defendant has wrongly stated that his use of AFR does not involve sensitive processing of a person's data unless they are on a watchlist of images against which the captured facial biometrics are compared (D-DG § 75). In this regard, the Claimant agrees with and adopts the submissions made on behalf of the Information Commissioner to the effect that the processing of biometric data of persons who are not on a watchlist still amounts to sensitive processing (IC § 16-18).

88. The Defendant's analysis of the law is wrong for the following reasons:

    (1) AFR is, by definition, deployed for the purposes of identifying "an" individual. It is used to identify whether one or more of the persons on a watchlist is present in a particular place at a particular time. The fact that such processing may ultimately determine that the Claimant (or any other individual whose facial biometrics are captured) is not an individual on the relevant watchlist would not prevent the purpose of the data processing being one of identification of individual(s) on that watchlist. Negative identification is as much identification as positive identification.

    (2) Consideration of three examples illustrates the flaws in the Defendant's reasoning. First, suppose two individuals are asked to take a DNA test to establish the paternity of a child. One is found to be the father and the other is not. On the Defendant's analysis, only the processing of the DNA of the former was "sensitive processing". That is plainly wrong. Second, and similarly, if AFR were used in respect of a small group of people to identify a single suspect, there could be no doubt that the processing would be "for the purpose" of identifying "an individual". Such processing would undoubtedly amount to (sensitive) processing of the biometric personal data of each member of the small group concerned. Logically, the same reasoning must apply to a group of 20,000 people. Third, if the police were to take the DNA of every person in a very large crowd for the purposes of locating several hundred suspects, there could be no doubt that they were processing the sensitive data of each person whose DNA was taken. If this is true of one major category of

biometrics it must be true of facial biometrics.

89. Given that the use of AFR amounts to sensitive processing, such processing will only be lawful if it satisfies three conditions:

    (1) It is "*strictly necessary for the law enforcement purpose*" (section 35(5) of the DPA 2018). The ICO's *Guide to Law Enforcement Processing* (April 2018, p.7) provides that: "*strictly necessary in this context means that the processing has to relate to a pressing social need,* [which cannot reasonably be achieved] *through less intrusive means. This is a requirement which will not be met if [the data controller] can achieve the purpose by some other reasonable means*".

    (2) It meets at least one of the conditions in Schedule 8 of the DPA 2018. The Claimant respectfully agrees with the Information Commissioner that the only condition with potential application is contained in paragraph 1 of Schedule 8 which relates to processing for the exercise of a function conferred on a person by an enactment or rule of law (see paragraph 37 above) [IC § 23].

    (3) At the time when the processing is carried out, the controller has an "appropriate policy document" in place, within the meaning of section 42 of the DPA 2018 (see paragraph 38 above).

90. As AFR is currently used by the Defendant, his sensitive processing of the biometric data of persons not included on a watchlist breaches section 35:

    (1) For the reasons set out above (see paragraph 74), the processing of a person's sensitive data cannot be characterised as "strictly necessary" for the law enforcement purpose(s) on which he relies.

    (2) To the extent that such processing could properly be described as necessary for the exercise of any of the Defendant's functions, it is not necessary for reasons of substantial public interest (to the extent that the Defendant relies on the condition in paragraph 1 of Schedule 8 to the DPA 2018). To the contrary, there is a strong public interest in the Defendant not gathering and processing the biometric data of very large numbers of innocent persons, which is not outweighed by the law enforcement benefits of the relevant deployments.

    (3) The document relied on as a purportedly "appropriate policy document" [HB2/F/17] for the purpose of section 42 of the DPA 2018 is fundamentally flawed because it is based on the misunderstanding that the use of AFR does

not involve "sensitive processing" in respect of the biometric data of persons who are not on watchlists.

GROUND 3C: BREACH OF THE OBLIGATION TO UNDERTAKE A DATA PROTECTION IMPACT ASSESSMENT

91. The DPA 2018 requires data controllers engaged in data processing for law enforcement purposes in circumstances such as the present to undertake a data protection impact assessment. Under the heading "General obligations", section 64 provides that:

> *(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the* ***controller must, prior to the processing, carry out a data protection impact assessment****.*
>
> *(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.*
>
> *(3) A data protection impact assessment must include the following –*
>
> > *(a) a general 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 this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.*
>
> *(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing*. (emphasis added)

The factual position

92. The Defendant prepared a privacy impact assessment in February 2018. This was produced prior to the entry into force of the DPA 2018 and, unsurprisingly, is not stated to have discharged the DPIA obligation (there was no such requirement under the DPA 1998).

93. It is said on behalf of the Defendant that an "updated assessment" has since been prepared (D-DG § 80). This appears to be the document entitled "DRAFT South Wales Police Data

Protection Impact Assessment" (version 5.4, dated 11 October 2018)[15] [HB2/F/16] which was lodged with the Defendant's Detailed Grounds. As such, the Defendant has accepted that AFR involves data processing that is likely to result in a high risk to the rights and freedoms of individuals.

Submissions

94. The Defendant is in breach of his obligation under section 64 of the DPA 2018. That is because in the completion of his DPIA he made a number of significant errors of law.

95. First, the DPIA fails to acknowledge that (a) the use of AFR entails the processing of the personal data of the many thousands of persons whose facial biometrics are captured through AFR but who are not on watchlists, and (b) the processing of these persons' data involves "sensitive processing" within the meaning of section 35 of the DPA 2018. This misdirection as to the nature of the processing involved (which chimes with the approach taken by the Defendant in this claim) necessarily means that in relation to people who are not on watchlists, the DPIA: (a) contains no proper assessment of the risks to their data protection rights; and (b) fails to set out measures to address those risks which are commensurate with the data in question being sensitive data.

96. Second, consistent with the Defendant's position in this litigation, the DPIA contains no acknowledgement that the use of AFR engages the Article 8 rights of persons whose facial biometrics are captured and processed but who are not on a watchlist. The consequence of this misdirection in law is that the DPIA does not assess the risks to the privacy rights of those data subjects. The DPIA shows no recognition that the collection, without consent, of the biometric data of vast numbers of people who are not suspected of any wrongdoing, and not on any watchlist, presents serious issues from a privacy point of view. Contrary to section 64(3) of the DPA 2018 the DPIA therefore contains no proper "*assessment of the risks to the rights and freedoms of [those] data subjects"* not on a watchlist through the use of AFR (section 64(3)(b)), nor does it include safeguards which take into account such individuals' "*rights and legitimate interests*" (section 64(3)(d)).

[15] The Defendant confirmed in correspondence on 15 January 2019 [HB2/H/8/56] that this version is the current version – the Claimant has not been made aware of any further iterations of this draft.

97. Finally, to the extent that there was no DPIA in place after 25 May 2018 and before October 2018, the Defendant is also in breach of section 64 on this basis.

GROUND 4: BREACH OF THE PUBLIC SECTOR EQUALITY DUTY

98. The Defendant has breached the PSED in respect of his ongoing use of AFR.

Legal principles

99. Section 149 of the Equality Act 2010 (**"EqA 2010**"), the PSED, provides so far as is relevant that:

> *(1) A public authority must, in the exercise of its functions, have due regard to the need to –*
>
> *(a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*
>
> *(b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

100. The principles applicable to the discharge of the PSED were summarised by McCombe LJ in Bracking v Secretary of State for Work and Pensions [2013] EWCA Civ 1345 at [25]; (which summary was endorsed by the Supreme Court in Hotak v Southwark LBC [2016] AC 811 at [73] per Lord Neuberger). So far as is relevant the applicable principles include:

(1) "*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", following a concluded decision…*" (Bracking at [25(4)]).

(2) The PSED includes a duty of inquiry. In Bracking, McCombe J at [26(8)(ii)] quoted from Elias LJ in R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills [2012] EWHC 20 at [89]: "*the duty of due regard … 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.*"

(3) The duty must be exercised "*in substance, with rigour, and with an open mind*". It is not a question of "*ticking boxes*" (Bracking at [25(5)]; see also R (Brown) v Secretary of State for Work and Pensions [2008] EWHC 3158 (Admin)). Moreover, it is insufficient for the decision maker to have a vague awareness of his legal

duties. Rather, they must have a focussed awareness of each of the constituent elements of the PSED and their potential impact on the relevant group (*R (MA) v Secretary of State for Work and Pensions* [2014] EWCA Civ 13 at [91] per Lord Dyson MR).

(4) What matters, for the purposes of compliance with the PSED, is *"what [the decision maker] took into account and what he or she knew"* (*Bracking* at [25]).

(5) 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]). As Simler J explained in *R(Blake) v Waltham Forest LBC* [2014] EWHC 1027 at [60]: having "*recognised and identified a potentially affected vulnerable group*," the decision maker must ensure "*negative impacts [are] … fully and frankly identified so the decision-maker can fully consider their impact*".

101. While it is for the decision maker to determine how much weight to give to the duty, 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). Provided that there has been "*a proper and conscientious focus on the statutory criteria*", the court "*cannot interfere … simply because it would have given greater weight to the equality implications of the decision*." But the decision maker must *"be clear precisely what the equality implications are"* (*Hurley and Moore* at [78] per Elias LJ).

The factual position

102. In order to comply with the PSED, a decision maker will need to consider whether measures they take may disadvantage those with protected characteristics. Often that is done by undertaking an Equality Impact Assessment of a policy or practice. Quite properly, an assessment was completed by the Defendant before it began using AFR. The Defendant completed an Initial Assessment ("**the EIA**") on 13 April 2017 [HB2/F/3]. More than two years later, this document appears to be the EIA on which the Defendant relies (though he stated in correspondence that a review of the EIA would be completed sometime after May 2019 [HB2/H/8/60]).

103. Again, quite properly the EIA asks whether there are any "concerns" that the AFR technology deployed by the Defendant "*could have a differential impact on racial groups*" (emphasis in original). The answer given is "*No*". This is said to be because:

> *AFR does not define race of an individual. When a person is potentially identified through the system. The identification is made on the match between the person's eyes and is based on algorithm matches. The camera does not define race or sex of an individual* [HB2/F/3/27-28].

The EIA gives a similar answer to the question of whether there is a differential impact on gender [HB2/F/3/28].

104. It is apparent from the EIA that 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 by the Defendant to whether AFR might operate in an indirectly discriminatory manner. The Defendant did not therefore ask himself whether AFR, although applied equally to white and non-white people and to men and women, might disadvantage those who were non-white or female because it is significantly more likely to generate false positives in respect of those people. As set out below that is based on a misdirection as to how discrimination law operates and it is fatal to the discharge of the PSED.

105. The failure to consider the risk of indirect discrimination is notwithstanding the ample coverage of concerns about the potential equalities implications of AFR in the media,[16] reports of NGOs[17] and in the academic literature (cited in Dr Jain's reports [HB1/E/1-2]). It is well established that "bias" is a common feature of AFR technology generally, irrespective of whether the AFR system defines the sex or race of the individual (AJ2 § 15) [HB1/E/2/54]. Dr Jain has addressed the concerns surrounding higher error rates in respect of (i) women and (ii) black / non-white people in his two expert reports. He summarises the effect of two US academic studies relied on by the Claimant:

> "*[Their findings] imply that [AFR] systems will be worse at correctly identifying female and darker-skinned faces (even when they are not classifying by gender or race). Thus when generating matches between faces detected and images on a watchlist, AFR systems will have a higher error rate for women and people from black and ethnic minority groups*" (AJ2 § 16) [HB1/E/2/54].

[16] See the examples cited at paragraph 89 of the Claimant's Statement of Facts and Grounds.
[17] See in particular *Face off: The lawless growth of facial recognition in UK policing* published by Big Brother Watch in May 2018 [HB2/G/7].

106. The risk that there will be significant differences in error rates is not marginal or trivial. One paper cited by Dr Jain found that the error rate for dark-skinned women to be more than 40 times higher than for lighter-skinned men (with an error rate of 34.7% for the former and only 0.8% for the latter) (AJ2 § 16) [HB1/E/2/54]). As Dr Jain explains, while that study looked at AFR systems that classify image by gender and race, he considered that their findings "*can be applied to AFR systems in general*" (ibid).

107. Dr Jain's first report provides an account of how AFR systems are "trained" (AJ1 § 42-47 [HB1/E/1/9-10]). As he explains, there is considerable evidence that the dataset with which an AFR system is "trained" has important implications for whether or not that system will have "biases" in relation to groups with particular protected characteristics (AJ1 § 48-50 [HB1/E/1/10]; AJ2 § 14, 24-25 [HB1/E/2/55-56]). 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*" (AJ1 § 49, 24-25 [HB1/E/1/5 & 10). As such, examining the dataset on which the system was trained is likely to be critical to understanding the equality implications of an AFR system to ensure that it broadly reflects the population of the place where it is deployed (AJ1 § 51 [HB1/E/1/10]; AJ2 § 15, 26-28 [HB1/E/2/54 & 56]).

108. At no stage has the Defendant had access, nor will he be able to obtain access, to the dataset on which his system of AFR was/is "trained". This is because information as to that dataset is "*commercially sensitive*" (Roberts § 20 [HB1/D/1/4]). The consequence of this is that the Defendant does not know: (i) the source of the images in the dataset; (ii) the size of the dataset; (iii) the racial composition of the dataset; (iv) the gender composition of the dataset; and (v) the demographic make-up of the dataset as compared to that of SWP's police area. The absence of this information is plainly not remedied by Mr Roberts' (an employee of the AFR technology provider) assurances that the training data includes a "*wide spectrum of different ethnicities*" (Roberts § 21-24 [HB1/D/1/5]). As Dr Jain states in his second report, Mr Roberts' evidence is:

> "*not sufficient to be able to determine that the NeoFace Algorithm is not biased towards a particular demographic group and thus AFR Locate not discriminatory. To make this determination, a thorough evaluation needs to be done of the demographic composition of*

the NeoFace Algorithm training dataset. The Defendant was or ought reasonably to have been aware of these concerns at all material times" (AJ2 § 27) [HB1/E/2/56].

Submissions

109. If AFR is applied neutrally (i.e., equally to all persons without regard to protected characteristics) but has a disproportionately high rate of false positives in respect of persons with a particular protected characteristic (e.g., women or members of particular racial or ethnic groups) this would be sufficient to put them at a particular disadvantage compared to those not sharing their protected characteristics (e.g., men or white people). That is because it makes it more likely that those with protected characteristics will be erroneously stopped by the police in order to check whether they are suspected of a criminal offence or wanted on a warrant. The risks of AFR operating in such an indirectly discriminatory manner are well known.

110. As set out above, the Defendant nevertheless considered only the possibility of AFR being used in a *directly* discriminatory manner. That appears to be based on a misdirection of law i.e., that AFR would only have discriminatory impact if the technology was specifically targeted to identify people of a particular race or gender (i.e., a risk of direct discrimination). The Defendant therefore did not consider the risk of <u>indirect</u> discrimination. That led to the obviously erroneous conclusion that there are "*no … concerns*" that AFR "*could have a differential impact*" on grounds of race or sex. It meant the Defendant has not been "*clear precisely what the equality implications are*" (see <u>*Hurley and Moore*</u> cited above) of his use of AFR, nor has he "*fully appreciate*[d] *the impact on those [potentially] affected*" by it (<u>*Bracking*</u>). He has not therefore satisfied the PSED.

111. Nor has the Defendant satisfied the PSED's duty of inquiry by ensuring that he has "*acquired … relevant material … before taking a decision* [to use AFR]" (see <u>*Hurley and Moore*</u>). The risk of indirect discrimination against particular groups through the use of AFR is clearly something to which those using the technology should be aware. Broadly speaking, there are two ways in which information can be gathered on that risk: (i) by examining and analysing the dataset on which the system of AFR was trained to ascertain whether it is likely to cause higher rates of false positives in respect of groups with particular protected characteristics; and/or (ii) by directly testing the operation of AFR and

examining whether discrimination arises. The Defendant has not done the former and has taken a flawed approach to the latter.

112. The Defendant relies on the analysis/monitoring of PC Edgell (covering deployments between May 2017 and June 2018), the results of which are set out in a statement of 26 November 2018 [HB1/D/4]. This analysis appears to have been undertaken in response to the current litigation and long after AFR began to be used by the Defendant. Furthermore, PC Edgell has failed to ask the correct questions to enable a determination to be made of whether the Defendant's use of AFR has a discriminatory impact. PC Edgell concluded that he has seen "*no bias based on either gender or ethnicity*" in the AFR system used by the Defendant (Edgell § 26) [HB1/D/4/36], which analysis is relied on in the Detailed Grounds (D-DC § 86).

113. The Defendant says 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 the Defendant 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 (AJ2 § 35) [HB1/E/2/57]). That is the only way to know whether, *of the faces scanned* by the software, the system disproportionately generates false matches for people from black and other minority ethnic communities and/or on the basis of gender. Yet, as PC Edgell states in his statement, "*the identity of those who have passed the camera without generating an alert are unknown*" (Edgell § 14 [HB1/D/4/34]).

114. The point may be illustrated by a hypothetical example. Suppose the Defendant applied the technology to a room of 10 people, eight of whom were white, and two of whom were not. Suppose further that the system generated four matches: two white, and two non-white; each of which is 50% accurate (that is to say, one white person was incorrectly matched, and one non-white person was incorrectly matched). The Defendant's approach is to compare the fact that 50% of false positives are non-white and 50% of true positives are non-white to draw the conclusion that the system is not biased.

In fact in those circumstances AFR would be showing significant bias. Of the white faces scanned, 12.5% were incorrectly matched, but of the non-white faces scanned 50% were incorrectly matched. The Defendant's approach to monitoring potential bias would miss entirely the actual evidence of the bias.

115. Far from providing evidence of his discharging the PSED, the Defendant's monitoring practices further reinforce the point that he has not appropriately comprehended and assessed the nature of the discrimination risk inherent in the technology. He has not therefore had due regard to the matters set out in the PSED.

116. The Defendant's failure to have due regard to the potential for his use of AFR to give rise to indirect discrimination is also apparent in his response to concerns relating to the amendment of threshold values. In his Detailed Grounds he avers in response to that concern that he does not set different threshold values for "*different genders or racial groups*" as this would be direct discrimination (D-DG § 87). That is not the only risk with altering threshold values. The risk is that if the threshold value is lowered for a person who happens to be of a particular racial group (not because of any discriminatory intent but because the police have a particular wish to apprehend that individual) that is likely to lead to significantly higher false positives for other members of that group (AJ2 § 23) [HB1/E/2/55]. That risk too appears to be one the Defendant has not appreciated and therefore it cannot be said that he has had due regard to it.

E: STANDING

117. The Defendant conceded permission on all grounds and, alongside the Interested Party (IP-DG § 2), he has "welcomed" the "oversight" of the Court (D-DG § 3). In these circumstances his refusal to accept that the Claimant has standing (a) for the purposes of his Article 8 claim (D-DG § 67), (b) in respect of his claim that the Defendant's ongoing use of AFR is in breach of section 35 of the DPA 2018 (D-DG § 73), and possibly[18] (c) in respect of his challenge concerning the Defendant's failure properly to comply with the DPIA obligation under section 64 of the DPA 2018, is difficult to understand.

[18] The Defendant's position on this is not clear from his Detailed Grounds.

118. Further, in his response to the pre-action letter the Defendant not only conceded permission but he also stated that he would not challenge the Claimant's standing [HB2/H/2/16]; yet, in the same letter the Defendant disputed the fact that the Claimant is a "victim" within the meaning of section 7 of the HRA [HB2/H/2/16 & 31]. This is a non-sequitur because the test for victimhood is the test for standing in respect of applications for a judicial review raising HRA grounds.

119. In granting permission, the Court neither raised nor reserved any questions in respect of standing.

Human Rights Act 1998

120. Section 7(3) of the HRA sets out the test for standing in relation to Convention rights challenges brought by way of an application for judicial review. It stipulates that:

> *If the proceedings are brought on an application for judicial review, the applicant is to be taken to have a sufficient interest in relation to the unlawful act only if he is, or would be, a victim of that act.*

That section goes on to state that "*a person is a victim of an unlawful act only if he would be a victim for the purposes of Article 34 of the Convention if proceedings were brought in the European Court of Human Rights in respect of that act"* (section 7(7)).

121. For the purposes of his Article 8 claim in respect of the Defendant's use of AFR on 21 December 2017 and 27 March 2018, the Claimant asserts standing on the basis that it is to be inferred that his facial biometrics and image were captured and processed (he relies on the facts and matters set out at paragraphs 19-23 and 77).

122. As to the Defendant's continuing use of AFR, the Claimant has standing to bring a judicial review claim as a resident of the police area in which the police force is regularly using AFR in public places and at events of the sort that he attends. The Claimant falls squarely within the class of people who risk being directly affected by the Defendant's use of AFR. That is sufficient to pursue an HRA challenge. As Lord Reed held in *AXA General Insurance v HM Advocate* [2012] 1 AC 868:

> *"…It is necessary to bear in mind in the first place* ***that the Convention is concerned … to ensure that it guarantees rights that are practical and effective. The interpretation of the concept of a "victim" is correspondingly broad****: as the*

Strasbourg court has observed, an excessively formalistic interpretation of that concept would make protection of the rights guaranteed by the Convention ineffectual and illusory: Lizarraga v Spain (2004) 45 EHRR 1031, para 38. It is also well established that a person can claim to be a victim of a violation of the Convention in the absence of an individual measure of implementation: as the Strasbourg court stated in Burden v United Kingdom (2008) 47 EHRR 857, para 34, ***it is open to a person to contend that a law violates his rights, in the absence of an individual measure of implementation, if he is a member of a class of people who risk being directly affected by it.*** *…"* (at [111]) (emphasis added).

DPA 2018

123. As addressed above, the Claimant's complaints under the DPA 2018 are two-fold: (i) through his ongoing use of AFR the Defendant is operating an unlawful policy or practice which is in breach of section 35 of the DPA 2018 (Ground 3B); and (ii) the Defendant is in breach of his obligation to conduct a DPIA (Ground 3C). These are both matters in respect of which the test for *locus standi* is sufficiency of interest.

124. It is submitted that the Claimant has a sufficient interest in the matters complained of under Grounds 3B and 3C on the footing that (a) he resides in the Defendant's police area; (b) the Defendant continues to have recourse to AFR; and (c) the Claimant frequents events and public places at which the Defendant deploys AFR (Bridges § 17 [HB1/C/1/4]) and in any event there appears to be no limits on the places in which the Defendant may deploy AFR. His interest in ensuring that his biometric data is not processed in breach of data protection principles and without a lawful DPIA in place is self-evident. Unless he is to avoid any public place at which AFR might be used in the future (which would be impossible for him to predict given the lack of constraints on where AFR may be used), he risks being subject to it. Equally, as a resident of the police area and a rate payer, he has an obvious interest in ensuring that SWP comply with their data protection obligations.

125. In *AXA General*, Lords Reed and Hope, whilst dealing with the supervisory jurisdiction in Scottish law, gave authoritative guidance on standing in English public law in relation to cases where there is a wider public interest in the court determining the legality of a public authority's action. Lord Reed held:

> *"… In some contexts, it is appropriate to require an applicant for judicial review to demonstrate that he has a particular interest in the matter complained of: the type of interest which is relevant, and therefore required in order to have standing, will depend upon the particular context. In other situations, such as where the excess or abuse of power affects the public generally, insistence upon a particular interest could prevent the matter being brought before the court, and that in turn might disable the court from performing its function to protect the rule of law … What is to be regarded as sufficient interest to justify a particular applicant's bringing a particular application before the court, and thus as conferring standing, depends therefore upon the context, and in particular upon what will best serve the purposes of judicial review in that context"* (at [170]).

126. As Lord Hope explained in AXA General in relation to standing "*[a] personal interest need not be shown if the individual is acting in the public interest and can genuinely say that the issue directly affects the section of the public that he seeks to represent*" (at [63]). Subsequently in Walton v The Scottish Ministers [2013] PTSR 51 , Lord Reed explained both his and Lord Hope's analysis in AXA General:

> *"In AXA General …, this court clarified the approach which should be adopted to the question of standing to bring an application to the supervisory jurisdiction. In doing so, it intended to put an end to an unduly restrictive approach which had too often obstructed the proper administration of justice: an approach which presupposed that the only function of the court's supervisory jurisdiction was to redress individual grievances, and ignored its constitutional function of maintaining the rule of law"* (at [90]).

127. The case concerns a new policing technology that, with the assistance of the Interested Party, is being trialled by the Defendant. It has affected, and is likely to continue to affect, large numbers of people in the Defendant's police area. If rolled-out and used regularly by other police forces, it would mean vast numbers of individuals having their biometric data taken and further processed. As is demonstrated by the Information Commissioner's intervention in relation to this issue, there is an obvious public interest in the court determining whether such processing is consistent with the DPA 2018. Indeed it is understood that is what the Defendant meant when he stated that he "*welcomes the Court's independent oversight*" and conceded permission so that the issues of legal principle could

be determined. It is obviously inconsistent with that for the Defendant to also contend that the court should not consider whether his use of AFR since the DPA 2018 is consistent with the Act simply because the Claimant has not been able to show that his biometric data was processed during that period (in circumstances where the data of thousands will have been taken and processed).

128. If there is a properly arguable case that the manner in which the Defendant operates AFR is inconsistent with the data protection principles contained in the DPA 2018 and without a proper DPIA being in place, it is respectfully submitted that that should be considered by the court on its merits and that a "*restrictive approach*" to standing would be to "*disable the court from performing its function to protect the rule of law*" in an area of public importance and public interest.

E: CONCLUSION

129. For the reasons given above, the Claimant respectfully invites the Court to allow his application for judicial review.

DAN SQUIRES QC
AIDAN WILLS
MATRIX

MEGAN GOULDING
LIBERTY

30 April 2019