Neutral Citation Number: [2020] EWCA Civ 1058

Case No: C1/2019/2670

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION (ADMINISTRATIVE COURT)
CARDIFF DISTRICT REGISTRY
Haddon-Cave LJ and Swift J
[2019] EWHC 2341 (Admin)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 11/08/2020

Before :

THE MASTER OF THE ROLLS
THE PRESIDENT OF THE QUEEN'S BENCH DIVISION
and
LORD JUSTICE SINGH

- -

Between :

R (on the application of Edward BRIDGES)	**Appellant/ Claimant**
- and -	
THE CHIEF CONSTABLE OF SOUTH WALES POLICE	**Respondent/ Defendant**
- and	
THE SECRETARY OF STATE FOR THE HOME DEPARTMENT	**Interested Party**
-and-	
THE INFORMATION COMMISSIONER (1) **THE SURVEILLANCE CAMERA COMMISSIONER (2)** **THE POLICE AND CRIME COMMISSIONER FOR SOUTH WALES (3)**	**Interveners**

- -
- -

Dan Squires QC and **Aidan Wills** (instructed by **Liberty**) for the **Appellant**

Jason Beer QC and **Francesca Whitelaw** (instructed by **Special Legal Casework, South Wales Police**) for the **Respondent**
Richard O'Brien and **Thomas Yarrow** (instructed by **the Government Legal Department**) for the **Interested Party**
Gerry Facenna QC and **Eric Metcalfe** (instructed by **the Information Commissioner's Office**) for the **First Intervener**
Andrew Sharland QC and **Stephen Kosmin** (instructed by **the Government Legal Department**) for the **Second Intervener**
Fiona Barton QC (instructed by South Wales and Gwent Police Joint Legal Services) made written submissions for the **Third Intervener**

Hearing dates : 23-25 June 2020

- -

Approved Judgment

Sir Terence Etherton MR, Dame Victoria Sharp PQBD and Lord Justice Singh :

1. This appeal concerns the lawfulness of the use of live automated facial recognition technology ("AFR") by the South Wales Police Force ("SWP") in an ongoing trial using a system called AFR Locate. AFR Locate involves the deployment of surveillance cameras to capture digital images of members of the public, which are then processed and compared with digital images of persons on a watchlist compiled by SWP for the purpose of the deployment. On the facts of the present case, AFR Locate has been used in an overt manner. It was not deployed as a form of covert surveillance. For that reason it is common ground that this case does not raise issues that might otherwise arise under the Regulation of Investigatory Powers Act 2000.

2. The appeal is from the order dated 4 September 2019 of Haddon-Cave LJ and Swift J in the Divisional Court of the Queen's Bench Division dismissing the Appellant's claim for judicial review challenging the legality of the use of AFR Locate on two particular occasions and on an ongoing basis. The grounds of challenge were that AFR is not compatible with the right to respect for private life under Article 8 of the European Convention on Human Rights ("the Convention"), which is one of the Convention rights set out in Sch.1 to the Human Rights Act 1998 ("HRA"); data protection legislation; and the Public Sector Equality Duty ("PSED") in section 149 of the Equality Act 2010.

3. The Divisional Court recorded in its judgment the co-operative and helpful way in which the case had been presented on all sides in order to ascertain the court's early guidance as to the legal parameters and framework relating to AFR while it is still in its trial phase and before it is rolled out nationally. This appeal has been conducted on the same basis.

The Parties

4. The Appellant, Edward Bridges, who was the claimant in these proceedings, is a civil liberties campaigner who lives in Cardiff. He has been supported by Liberty, the well-known independent civil liberties membership organisation. The Respondent is the Chief Constable of SWP (*Heddlu De Cymru*).

5. The Interested Party, the Secretary of State for the Home Department, is responsible for policing nationwide and has concern for the development and lawful use of technology, such as AFR, which has the potential to assist in the prevention and detection of crime. The Secretary of State has provided funding to SWP to develop AFR and in June 2018 published the Home Office Biometrics Strategy. The Secretary of State created an Oversight and Advisory Board to co-ordinate consideration of the use of facial images and AFR technology by law enforcement authorities.

6. There are two interveners who were also interveners before the Divisional Court, the Information Commissioner and the Surveillance Camera Commissioner. The Information Commissioner has specific statutory powers and responsibilities under the Data Protection Act 2018 ("the DPA 2018"), and also had responsibilities under the predecessor legislation, the Data Protection Act 1998 ("the DPA 1998"). The Surveillance Camera Commissioner is the statutory regulator of surveillance cameras. He has specific powers and responsibilities under section 34 of the Protection of Freedoms Act 2012 ("the PFA 2012") with regard to encouraging compliance with the

Surveillance Camera Code of Practice, reviewing its operation and providing advice about the Code of Practice. His responsibilities include, in particular, regulating the use of surveillance cameras and their use in conjunction with AFR technology. In addition, this Court has received submissions (in writing only) on behalf of a third intervener, the Police and Crime Commissioner for South Wales.

AFR and its deployment by SWP

7. An impressive explanation of AFR and its deployment by SWP was given in considerable detail in the judgment of the Divisional Court. For a full account, reference should be made to that judgment at [23]-[40]. There has been no criticism of the accuracy of the Divisional Court's account. We have, therefore, gratefully taken what follows from their judgment.

AFR Technology

8. AFR is a way of assessing whether two facial images depict the same person. A digital photograph of a person's face is taken and processed to extract biometric data (*i.e.* measurements of the facial features). That data is then compared with facial biometric data from images contained in a database.

9. In more detail, the technical operation of AFR comprises the following six stages:

(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 in them. 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 CCTV camera takes digital pictures of facial images in real time. This case is concerned with the situation where a moving image is captured when a person passes into the camera's field of view, using a live feed.

(3) Face detection. Once a CCTV camera used in a live context captures footage, the software (a) detects human faces and then (b) 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, the resulting biometric template being unique to that image.

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

(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. A threshold value is fixed to determine when the software will indicate that a match has occurred. 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). The threshold value is generally suggested by the manufacturer, and depends on the intended use of the AFR system. Most AFR systems, however, allow the end user to change the threshold value to whatever they choose.

SWP's use of AFR

10. SWP is the police authority which is the national lead on testing and conducting trials of AFR. SWP has a licence to use proprietary AFR software developed by NEC (now North Gate Public Services (UK) Ltd) called "NeoFace Watch software".

11. SWP uses AFR in two ways. We are concerned in this appeal only with the use of the AFR system which SWP calls "AFR Locate". SWP deployed AFR Locate on about 50 occasions between May 2017 and April 2019 at a variety of large public events.

12. When AFR Locate is deployed SWP mounts CCTV cameras on police vehicles, or on poles or posts, so as to capture images of the face of anyone who passes within range of the camera. As we have described above, digital images of faces of members of the public are taken from the CCTV feeds and processed in real time to extract facial biometric information. That information is then compared with facial biometric information of persons on a watchlist prepared for the purpose of that specific deployment.

13. The watchlist is created from images held on databases maintained by SWP as part of its ordinary policing activities, primarily from a database of custody photographs held on SWP's Niche Record Management System. The images selected for inclusion on a watchlist will depend on the purpose of each specific deployment. The watchlists used in the deployments in issue in this case have included (1) persons wanted on warrants, (2) individuals who are unlawfully at large (having escaped from lawful custody), (3) persons suspected of having committed crimes, (4) persons who may be in need of protection (*e.g.* missing persons), (5) individuals whose presence at a particular event causes particular concern, (6) persons simply of possible interest to SWP for intelligence purposes and (7) vulnerable persons. To date, the watchlists used by SWP have comprised between 400-800 people. The maximum capacity for a watchlist is 2,000 images but, as we understand it, this is because of the limits of the technology used rather than any limitation of principle.

14. As described above, a biometric template is taken from the images on the watchlist which will then be used for the purposes of undertaking algorithmic comparisons with the facial biometrics of members of the public captured on camera.

15. If, during a deployment of AFR Locate, the software identifies a possible match between a face captured on the CCTV and an image on the watchlist, the two images are reviewed by an AFR operator ("the system operator", who is a police officer) to establish whether he or she believes that a match has in fact been made. If, upon reviewing the images of the person on the watchlist and the person whose image has been captured by CCTV, the system operator does not consider that they are the subject of interest, then no further action is taken. If, however, it is believed that there is a match, other officers stationed nearby may be notified, and they will intervene, for example by asking to speak to the person concerned and, if appropriate, using statutory powers to stop and search or arrest the person.

16. The CCTV camera records footage for the duration of any AFR Locate deployment. AFR Locate is capable of scanning 50 faces per second (although that does not necessarily mean 50 different people). Beyond those technical limitations, there is no limit on the number of persons who may have their facial biometrics captured during any given deployment. It is SWP's intention during each deployment to allow AFR Locate to process as many individuals as possible. It is clear that the numbers of persons processed are very large. Over the 50 deployments that were undertaken in 2017 and 2018, around 500,000 faces may have been scanned. The overwhelming majority of persons whose biometrics are captured and processed by SWP using AFR Locate are not suspected of any wrongdoing and are not otherwise of interest to the police.

Data retention

17. If no match (false or positive) is made – as in the overwhelming majority of cases – then AFR Locate does not retain the facial biometrics or image of persons whose faces are scanned. They are immediately and automatically deleted. That data is not available to the system operator or any other police officer. The CCTV feed is retained for 31 days in accordance with the standard CCTV retention period. Data associated with a match is retained within AFR Locate for up to 24 hours. In the event of no match, the data is immediately deleted.

18. SWP's Standard Operating Procedures and Data Protection Impact Assessment provide for data retention periods. These are kept under review. The current data retention periods are as follows:

    (1) CCTV feed to AFR Locate deployments: retained for 31 days with automatic deletion as part of the "Milestone" software.

    (2) Facial images that are not matched against: immediately deleted.

    (3) Biometric template (regardless whether match made): immediately deleted.

    (4) Facial images alerted against: images either deleted immediately following the deployment, or, at the latest, within 24 hours following the deployment.

    (5) Match report to include personal information (name of individual alerted against): retained for 31 days.

    (6) Watchlist images and related biometric template: deleted immediately following the deployment, or at the latest within 24 hours following the deployment.

Public awareness of when AFR Locate is used

19. When AFR is deployed, SWP take steps to inform members of the public about AFR and as to its use at the event or in the area in question. Those steps include the following: (1) prior to each AFR deployment, utilising Facebook and Twitter to advertise the deployment and its location and invite engagement with officers who are deploying the technology; (2) displaying large A2-size "Fair Processing Notices" on the AFR-equipped police vehicles on site and at approximately a 100 metre radius of the AFR cameras; and (3) handing out postcard-sized notices to members of the public in the

vicinity of each AFR deployment and to every person that is spoken to as a result of an AFR intervention. There is also material about AFR on SWP's website.

20. Whilst deployment of AFR is not covert, it is nevertheless reasonable to suppose that a large number of people whose facial biometrics are captured and processed by SWP's use of AFR are unaware of this taking place.

Biometric Data

21. The use of AFR technology involves the collection, processing and storage of a wide range of information, including (1) facial images; (2) facial features (*i.e.* biometric data); (3) metadata, including time and location, associated with the same; and (4) information as to matches with persons on a watchlist. AFR entails the processing of biometric data in the form of facial biometrics. The term "biometrics" is described in the Home Office "Biometrics Strategy – Better Public Services Maintaining Public Trust" published in June 2018 (para. 1) as "the recognition of people based on measurement and analysis of their biological characteristics or behavioural data".

22. Biometric data enables the unique identification of individuals with some accuracy. It is this which distinguishes it from many other forms of data. Facial biometrics are one of the primary forms of biometric data, alongside fingerprints and DNA.

23. Facial biometrics bear some similarity to fingerprints because both can be captured without the need for any form of intimate sampling and both concern a part of the body that is generally visible to the public. A significant difference, however, is that AFR technology enables facial biometrics to be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale.

Oversight and Advisory Board

24. The Secretary of State has set up an Oversight and Advisory Board, comprising representatives from the police, the Home Office, the Surveillance Camera Commissioner, the Information Commissioner, the Biometrics Commissioner, and the Forensic Science Regulator, to co-ordinate consideration of the use of facial imaging and AFR by law enforcement authorities.

The specific incidents giving rise to these proceedings

25. In addition to challenging the lawfulness of SWP's use of AFR Locate generally, the Appellant complains about two particular occasions when AFR Locate was used in Cardiff by SWP and, he maintains, he was caught on camera. Those two occasions were: (1) on 21 December 2017 at Queen Street, a busy shopping area in Cardiff; and (2) on 27 March 2018 at the Defence Procurement, Research, Technology and Exportability Exhibition ("the Defence Exhibition") which was held at the Motorpoint Arena.

21 December 2017 Deployment

26. On 21 December 2017 SWP deployed a single marked AFR-equipped van at Queen Street in Cardiff city centre. The AFR system was live from 8:00 am to 4:00 pm. There were three watchlists for this deployment: one was of a person suspected of having committed a serious crime, another comprised 382 people wanted on warrants, and the

third comprised 536 suspects (in effect, every person suspected of committing a crime in SWP's area). There were ten possible matches during the deployment. Of these two were not true matches. In one of those cases there was no intervention. Of the eight true matches there were two arrests.

27. The Appellant says he was present at Queen Street on 21 December 2017, that he was approximately 6-10 feet from the van and that he was, accordingly, in range of the cameras. He states 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.

27 March 2018 deployment

28. On 27 March 2018 the Defence Exhibition took place at the Motorpoint Arena in Cardiff. In previous years the event had attracted disorder and persons involved in past protests had caused criminal damage and made two bomb hoax calls to disrupt the event. AFR was live between 8:30 am and 4:00 pm with the cameras focusing on the arena's entrance.

29. There were again three watchlists: one comprised subjects of interest who had been arrested at the same event the previous year, five of whom had been convicted of a variety of offences, another comprised 347 persons wanted on warrants, and the third comprised 161 suspects (linked to crimes in SWP's area ranging from summary only offences to the most serious indictable offences). No arrests were made during this deployment. There were no false alerts. There was one correct match: one of the six people who had been arrested the previous year was correctly identified as being at the event. She had made a false bomb report the previous year, and had been convicted of that offence and sentenced to a suspended sentence order of 18 months' imprisonment. The information that the offender was at the event was passed to the Event Commander, but no further action was taken.

30. The Appellant's evidence was that he attended a protest outside the Motorpoint Arena. He stated in his witness statement that he was 25-30 metres away from the AFR-equipped van, but at one point he would have been closer than that. He said that, prior to seeing the van, he was not aware that AFR was in use, and he did not observe SWP officers providing any information about the use of AFR.

Relevant legal framework

31. Relevant legal and other material is set out in the Annex to this judgment.

The proceedings

32. The claim was filed by the Appellant on 3 October 2018 and issued on 18 October 2018. It was accompanied by a detailed Statement of Facts and Grounds, in which it was stated that the Appellant challenged (1) the unlawful use of the technology against him on the two occasions mentioned above, and (2) SWP's ongoing use of AFR in public places in the police area in which he resides, giving rise to clear risk of the technology again being used against him. It was stated that the grounds for the challenge were (1) breach of Article 8 of the Convention; (2) breach of Articles 10 and 11 of the Convention; (3) breaches of data protection law, namely section 4(4) of the DPA 1998 taken with the first data protection principle in Schedule 1, section 35(1) of the DPA

2018 and section 64 of the DPA 2018; and (4) breach of the PSED. The Appellant sought declarations as to those breaches and damages.

33. In the event, ground 2 has not been pursued.

34. SWP has not challenged the Appellant's standing to bring these proceedings. It has not been possible for SWP to check either whether the Appellant's image was recorded by CCTV on 21 December 2017 or 27 March 2018 or whether his facial biometric information was processed by the AFR equipment on either occasion. For pragmatic reasons SWP has accepted the Appellant's evidence that he was present on both occasions and that on those occasions his image was recorded. SWP does not dispute that the Appellant is a victim for the purposes of section 7 of the HRA. Permission to apply for judicial review was granted by consent, SWP and the Secretary of State opposing the grounds for judicial review on the substantive merits.

The Divisional Court's judgment

35. The Divisional Court heard the claim over three days. It handed down an admirably clear and comprehensive judgment on 4 September 2019. It is impossible in the following brief summary to do justice to the judgment. We do no more than summarise the principal points of the judgment in order to provide a context for this appeal and our discussion and conclusions below.

Article 8 of the Convention

36. The Divisional Court held that Article 8 was engaged. They considered that, like fingerprints and DNA, AFR technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances, and that AFR-derived biometric data is information of an intrinsically private character. They said (at [57]) that the fact that the biometric data is derived from a person's facial features that are manifest in public does not detract from that. They said (at [59]) that Article 8 is triggered by the initial gathering of the information and that it is sufficient if biometric data is captured, stored and processed, even momentarily.

37. The Divisional Court found that the interference with rights in Article 8(1) was justified by the conditions of Article 8(2). They rejected the Appellant's primary argument that the use of AFR Locate by SWP was not "in accordance with the law" for the purposes of Article 8(2) because (1) there is no legal basis for the use of AFR Locate and so SWP does not, as a matter of law, have power to deploy it, and (2) in any event, any interference with Article 8 rights is not subject to a sufficient legal framework.

38. The Divisional Court held (at [75] to [78]) that using cameras with AFR technology to obtain the biometric data of members of the public in public falls within the common law powers of the police to obtain and store information for policing purposes, and that the compilation of the watchlists is both authorised under the Police and Criminal Evidence Act 1984 and within the powers of the police at common law. This is not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy AFR Locate.

39. Having cited the general principles summarised by Lord Sumption in *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9, [2015] AC 1065 at [11] to [14] and *R (P) v Secretary of State for Justice and Another* (also known as *In re Gallagher*) [2019] UKSC 3, [2020] AC 185, at [16] to [31] applicable to the "in accordance with the law" standard for the purposes of Article 8(2), the Divisional Court held (at [84]) that there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used, comprising (in addition to the common law): (1) primary legislation, (2) secondary legislative instruments in the form of codes of practice issued under primary legislation, and (3) SWP's own local policies.

40. As to primary legislation, the Divisional Court referred to the DPA 2018 (which they said they focused on rather than the DPA 1998 only for the sake of convenience). They said (at [85]) that it embeds key safeguards which apply to all processing of personal data, including the biometric data processed when AFR Locate is used. They referred, in particular, to the provisions in Part 3 of the DPA 2018. They observed (at [88]) that the requirements arising under the DPA 2018 are mirrored in the Code of Practice on the Management of Police Information, issued by the College of Policing under section 39A of the Police Act 1996, and that section 39A(7) of the 1996 Act requires chief police officers to have regard to that Code.

41. As to the second element of the framework, the Divisional Court said (at [91]) that they agreed with the overall submission of the Surveillance Camera Commissioner that the Surveillance Camera Code of Practice, issued by the Home Secretary pursuant to section 30 of the PFA 2012 and to which a chief officer of police must have regard, provides a full system approach to the regulation of surveillance camera systems, as it provides the legal and good practice standard which the Government expects, as well as highlighting the broader spectrum of legislative requirements which apply.

42. As to the third element of the framework, SWP's own policies as to the use of AFR Locate, the Divisional Court said (at [92]) that the three relevant policies are (1) SWP's Standard Operating Procedure, (2) SWP's Deployment Reports and (3) SWP's Policy on Sensitive Processing.

43. The Divisional Court concluded (at [96]) that, drawing everything together, the cumulative effect of (1) the provisions of the DPA, (2) the Surveillance Camera Code of Practice and (3) SWP's own policy documents, is that the interference with the rights in Article 8(1) which is consequent on SWP's use of AFR Locate, occurs within a legal framework that is sufficient to satisfy the "in accordance with the law" requirement in Article 8(2); and that the answer to the primary submissions of the Appellant (and the Information Commissioner who supported him on this issue) is that it is neither necessary nor practical for legislation to define the precise circumstances in which AFR Locate may be used, *e.g.* to the extent of identifying precisely which offences might justify inclusion on a watchlist as a subject of interest or precisely what the sensitivity settings should be.

44. The Divisional Court then turned to the question of whether the interference of AFR Locate with Article 8(1) satisfied the four-part proportionality test in *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39, [2014] AC 700. Having accepted that it was appropriate, when applying the third and fourth criteria in the context of the facts of the present case, to apply a close standard of scrutiny, the Divisional Court rejected all the substantive submissions of the Appellant on this issue. They concluded (at [101])

that the use of AFR Locate on 21 December 2017 (Queen Street) and 27 March 2018 (Motorpoint Arena) struck a fair balance and was not disproportionate. The Divisional Court further said (at 108]), regarding any future use of AFR Locate, that, on the evidence before them as to the manner in which AFR Locate was currently deployed by SWP, they were satisfied that there is no systemic "proportionality deficit" such that it can be said that future use of AFR Locate by SWP would be inevitably disproportionate.

Data Protection claims

45. The Divisional Court recorded (at [109]) that, although none of the deployments by SWP of AFR in issue in the proceedings took place after the commencement of the DPA 2018 (25 May 2018), all parties had requested that the legality of the deployments of AFR Locate be considered as if they had taken place after 25 May 2018 and the Divisional Court were content to do so. The Divisional Court addressed the data protection claims under three headings: (1) the claim under the DPA 1998, (2) the claim under section 35 of the DPA 2018, and (3) the claim under section 64 of the DPA 2018.

46. The primary point of dispute before the Divisional Court under the DPA 1998 was the extent to which using AFR Locate entails processing personal data, SWP contending that the only personal data processed is the data of persons on the watchlist on the ground that it is only those persons that SWP can identify by name. Having referred to the judgment of the Court of Appeal in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003, and to the decision of the CJEU in Case C-212/13 *Rynes v Urad* [2015] 1 WLR 2607, the Divisional Court concluded (at [122]) that the processing of the Appellant's image by the AFR Locate equipment was processing his personal data because the information recorded by AFR Locate individuated him from all others, that is to say it singled him out and distinguished him from all others.

47. The Divisional Court rejected, however, the Appellant's case that SWP acted unlawfully under section 4(4) of the DPA 1998 by failing to comply with the first data protection principle, in particular that personal data must be processed lawfully and fairly. Given their conclusion on the Appellant's Article 8 claim, the Divisional Court were satisfied that the use of AFR Locate in December 2017 and March 2018 satisfied that condition of lawfulness and fairness.

48. Turning to the requirement in section 34 of the DPA 2018 that SWP, as a "competent authority", had to be able to demonstrate compliance with the provisions of Chapter 2 of Part 3 of the DPA 2018 concerning law enforcement processing, the Divisional Court identified the issues in dispute as being: (1) whether (as the Appellant contended but SWP contested) the processing of the biometric data of members of the public whose faces are captured by the CCTV cameras entails "sensitive processing" as described in section 35(8) of the DPA 2018, and (2) whether (as the Appellant contended but SWP contested) AFR Locate failed to meet the requirements of section 35(5). Those requirements are that: (a) the processing is strictly necessary for a 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. The Appellant contended that none of those requirements was satisfied.

49. On the first issue, the Divisional Court concluded (at [132] and [133]) that AFR Locate does entail sensitive processing within section 35(8) insofar as it involves processing biometric data of members of the public "for the purpose of uniquely identifying an individual" within section 35(8)(b).

50. On the second issue, the Divisional Court found that AFR Locate meets the first requirement of section 35(5). They held (at [136]) that, for all the reasons given by them in relation to proportionality in the context of Article 8, the first of the requirements at section 35(5), namely "the processing is strictly necessary for the law enforcement purpose", was satisfied. The Divisional Court held (at [137]) that the second requirement of section 35(5), that the processing must meet at least one of the conditions in Schedule 8 to the DPA 2018, was satisfied because of compliance with paragraph 1 of Schedule 8, the processing being necessary for the reasons given by the Divisional Court in the context of proportionality and Article 8, and the relevant rule of law being the common law duty to prevent and detect crime. As to the third requirement, that the controller has an appropriate policy document in place in relation to the sensitive processing in accordance with section 42, the Divisional Court said (at [139]) that they thought it was open to question whether the policy document relied upon by SWP, entitled "Policy on Sensitive Processing for Law Enforcement Purposes" dated November 2018 ("the November 2018 Policy Document"), fully met the standard required by section 42(2). They added the following at [141]:

> "For the moment, we confine ourselves to the above observations. Given the role of the Information Commissioner and the prospect of further guidance, we do not think it is necessary or desirable for this Court to interfere at the present juncture and decide whether the SWP's current November 2018 Policy Document meets the requirements of section 42(2) of the DPA 2018. In our view, the development and specific content of that document is, for now, better left for reconsideration by the SWP in the light of further guidance from the Information Commissioner."

51. The Divisional Court turned finally, in respect of the Appellant's data protection claims, to his claim that SWP had failed to comply with the obligation to undertake an impact assessment complying with section 64 of the DPA 2018. The Divisional Court rejected that claim on the grounds that at all material times the processing by SWP was supported by a relevant data protection impact assessment ("DPIA") and that, approaching the matter on the footing that SWP had brought to bear a conscientious assessment, the impact assessment prepared by SWP did meet the requirements of section 64.

The PSED claim

52. The Divisional Court rejected the Appellant's claim that SWP had failed to comply with its obligation under section 149 of the Equality Act 2010 because it did not, in its assessment, consider the possibility that AFR Locate might produce results that were indirectly discriminatory on grounds of sex and/or race because it produces a higher rate of positive matches for female faces and/or for black and minority ethnic faces. The Divisional Court said (at [153]) that there was no suggestion that, as at April 2017

when the AFR Locate trial commenced, SWP either recognised or ought to have recognised that the NeoFace Watch software it had licensed might operate in a way that was indirectly discriminatory, and even at the date of the hearing there was no firm evidence that the software did produce results that suggested indirect discrimination. The Divisional Court concluded (at [158]) that the Equality Impact Assessment prepared by SWP in April 2017 demonstrated that due regard was had by SWP to the section 149(1) matters.

The appeal

53. Permission to appeal has been given for all the following five grounds of appeal for which permission was sought:

Ground 1: The Divisional Court erred in concluding that the interference with the Appellant's rights under Article 8(1) of the Convention, taken with section 6 of the HRA 1998, occasioned by SWP's use of AFR on 21 December 2017 and 27 March 2018 and on an ongoing basis, was/is in accordance with the law for the purposes of Article 8(2).

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

Ground 3: The Divisional Court was wrong to hold that SWP's DPIA complied with the requirements of section 64 of the DPA 2018. The DPIA is based on two material errors of law concerning the (non)engagement of the rights in Article 8 of the Convention and the processing of the (biometric) personal data of persons whose facial biometrics are captured by AFR but who are not on police watchlists used for AFR.

Ground 4: The Divisional Court erred in declining to reach a conclusion as to whether SWP has in place an "appropriate policy document" within the meaning of section 42 of the DPA 2018 (taken with section 35(5) of the DPA 2018), which complies with the requirements of that section. Having in place such a document is a condition precedent for compliance with the first data protection principle (lawful and fair processing) contained in section 35 of the DPA 2018 where the processing of personal data constitutes "sensitive processing" within the meaning of section 35(8) of the DPA.

Ground 5: The Divisional Court was wrong to hold that SWP complied with the PSED in circumstances in which SWP's Equality Impact Assessment was obviously inadequate and was based on an error of law (failing to recognise the risk of indirect discrimination) and SWP's subsequent approach to assessing possible indirect discrimination arising from the use of AFR is flawed. It is argued that the Divisional Court failed in its reasoning to appreciate that the PSED is a continuing duty.

Discussion

Ground 1: Sufficient Legal Framework

54. The Divisional Court addressed what is now the subject of Ground 1 in this appeal at [79]-[97] of its judgment, where it asked the question: "Is there a sufficient legal framework for the use of AFR Locate?"

55. The Divisional Court set out the general principles on this issue at [80]:

> "The general principles applicable to the 'in accordance with the law' standard are well-established: see generally per Lord Sumption in *Catt*, above, [11]-[14]; and in *Re Gallagher* [2019] 2 WLR 509 at [16] – [31]. In summary, the following points apply.
>
> (1) The measure in question (a) must have 'some basis in domestic law' and (b) must be 'compatible with the rule of law', which means that it should comply with the twin requirements of 'accessibility' and 'foreseeability' (*Sunday Times v United Kingdom* (1979) 2 EHRR 245; *Sliver v United Kingdom* (1983) 5 EHRR 347; and *Malone v United Kingdom* (1984) 7 EHRR 14).
>
> (2) 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. 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' (Lord Sumption in *Re Gallagher, ibid,* at [17]).
>
> (3) Related to (2), the law must 'afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise' (*S v United Kingdom,* above*,* at [95] and [99]).
>
> (4) Where the impugned measure is a discretionary power, (a) what is not required is 'an over-rigid regime which does not contain the flexibility which is needed to avoid an unjustified interference with a fundamental right' and (b) 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' (per Lord Hughes in *Beghal v Director of Public Prosecutions* [2016] AC 88 at [31] and [32]). Any exercise of power that is unrestrained by law is not 'in accordance with the law'.

> (5) The rules governing the scope and application of measures need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them (*per* Lord Sumption in *Catt* at [11]).
>
> (6) The requirement for reasonable predictability does not mean that the law has to codify answers to every possible issue (*per* Lord Sumption in *Catt* at [11]).”

56. There was no material dispute between the parties before this Court that that was an accurate statement of the relevant principles. In applying those principles to the present context, the Divisional Court concluded as follows, at [84]:

> “In our view, there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used. … The legal framework within which AFR Locate operates comprises three elements or layers (in addition to the common law), namely: (a) primary legislation; (b) secondary legislative instruments in the form of codes of practice issued under primary legislation; and (c) SWP's own local policies. Each element provides legally enforceable standards. When these elements are considered collectively against the backdrop of the common law, the use of AFR Locate by SWP is sufficiently foreseeable and accessible for the purpose of the ‘in accordance with the law’ standard.”

57. The Divisional Court considered the legislation and policy documents and concluded as follows, at [96]-[97]:

> “96. Drawing these matters together, the cumulative effect of (a) the provisions of the DPA, (b) the Surveillance Camera Code and (c) SWP's own policy documents, is that the infringement of Article 8(1) rights which is consequent on SWP's use of AFR Locate, occurs within a legal framework that is sufficient to satisfy the ‘in accordance with the law’ requirement in Article 8(2). The answer to the primary submissions of the Claimant and the Information Commissioner, is that it is neither necessary nor practical for legislation to define the precise circumstances in which AFR Locate may be used, *e.g.* to the extent of identifying precisely which offences might justify inclusion as a subject of interest or precisely what the sensitivity settings should be (*c.f.* Lord Sumption in *Catt* at [14]). Taking these matters as examples, the Data Protection Principles provide sufficient regulatory control to avoid arbitrary interferences with Article 8 rights. The legal framework that we have summarised does provide a level of certainty and foreseeability that is sufficient to satisfy the tenets of Article 8(2). It provides clear legal standards to which SWP will be held. As to the content of local policies, we take account that AFR Locate is still in a trial period. The

> content of SWP's policies may be altered and improved over the course of this trial. The possibility (or even the likelihood) of such improvement is not evidence of present deficiency.
>
> 97. Finally, under this heading, we refer to the comments by the Home Secretary (in her Biometrics Strategy) as to the legal framework within which AFR Locate presently operates (see above, at paragraph 67). In our view, when considered in context, these comments should be considered as amounting to pragmatic recognition that (a) steps could, and perhaps should, be taken further to codify the relevant legal standards; and (b) the future development of AFR technology is likely to require periodic re-evaluation of the sufficiency of the legal regime. We respectfully endorse both sentiments, in particular the latter. For the reasons we have set out already, we do not consider that the legal framework is at present out of kilter; yet this will inevitably have to be a matter that is subject to periodic review in the future."

58. We find the references by the Court to the possibility of future reconsideration of this issue a little curious. This is because either an interference is in accordance with the law or it is not. The issue of whether there is relevant "law" for this purpose is a binary question: see *In re Gallagher*, at [14] (Lord Sumption JSC). The fact that this case involved the trial of a new technology does not alter the need for any interference with Article 8 rights to be in accordance with the law.

59. Mr Squires QC invited us to have regard to hypothetical scenarios which may arise in the future, for example if the large network of CCTV cameras in this country were to be connected to AFR Locate in such a way that a person's movements around the country could be tracked. In support of that submission Mr Squires urged upon us what was said in the dissenting judgment of Lord Kerr JSC in *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88, at [93] and [102]. In that last paragraph, Lord Kerr said that:

> "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." (Emphasis added)

60. Apart from the fact that Lord Kerr's was a dissenting judgment, there is always a danger of reading what a judge says in a particular case as if it were a provision of general application in a statute. We do not accept that, in the present case, it is either necessary or helpful to consider hypothetical scenarios which may arise in the future, as Mr Squires urged us to do. We consider that what must be examined is the particular interference with Article 8 rights which has arisen in this present case and in particular whether that interference is in accordance with the law. Whether other uses of police power in other contexts will be lawful in the future will be a matter to be considered if the facts of such a case arise in practice. This is consistent with the approach of the

European Court of Human Rights, which usually asks whether there has been a violation of an applicant's rights on the particular facts of the case before it. As Lord Bingham of Cornhill said in *Brown v Stott* [2003] 1 AC 681, at 704:

> "The case law shows that the court has paid very close attention to the facts of particular cases coming before it, giving effect to factual differences and recognising differences of degree."

61. We also accept the submission made in particular by Mr Sharland QC, on behalf of the Surveillance Camera Commissioner, that what is in issue in this appeal is the local deployment of AFR within the area of SWP. This appeal is not concerned with possible use of AFR in the future on a national basis. As Mr Sharland submits, it is well-established in the caselaw of the European Court of Human Rights that local policies can be relevant to satisfy the requirement of "in accordance with the law". Such policies do not necessarily have to be at a national level. He cited the decision of the European Court of Human Rights in *Munjaz v United Kingdom* [2012] MHLR 351, at [83]-[95]. In that case what was in issue was the policy on seclusion of patients at a "special hospital", Ashworth, which was a high security hospital. The European Court of Human Rights concluded that the hospital's policy of seclusion did give sufficient indication of the scope of discretion which the hospital enjoyed and that the manner of that discretion was exercised with sufficient clarity to protect the applicant against arbitrary interference with his Article 8 rights.

62. Particular reliance was placed by Mr Facenna QC, on behalf of the Information Commissioner, on the decision of the Court of Justice of the European Union in *Tele2 Sverige AB v Post-och telestyrelsen* and *R (Watson) v Secretary of State for the Home Department* (joint cases C-203/15 and C-698/15) [2017] QB 771. That case, so far as it concerned the UK, concerned the compatibility of the Data Retention and Investigatory Powers Act 2014 with EU law, including the Charter of Fundamental Rights. Article 7 of that Charter contains a guarantee which is similar to Article 8 of the Convention. The legislation empowered the Secretary of State to issue a "retention notice" on a public telecommunications operator to retain "relevant communications data" if the Secretary of State considered that the requirement was necessary and proportionate for one or more of the purposes specified in the legislation. This in effect permitted the large scale and indiscriminate retention of electronic communications data of members of the public. Although this did not include the *content* of communications, it did include much other personal data, sometimes called "metadata": it would be possible, for example, to trace and identify the source of a communication; the date, time, duration and type of communication; and the location of mobile communications equipment (see [98]).

63. The Court of Justice laid down a series of strict and detailed conditions for the compatibility of such intrusive legislation with EU law: see [102]-[122]. For example, at [120], the Court said that what was required in that context, except in cases of urgency, was "a prior review carried out either by a court or by an independent administrative body".

64. We consider, however, that the Court's reasoning was principally directed to the question of proportionality rather than the requirement that an interference with rights must be in accordance with the law. Secondly, it was concerned with the specific

requirements of EU law: see *e.g.* [117], which cited the specific terms of Directive 2002/58, which expressly refers to a measure having to "be subject to adequate safeguards". Thirdly, that case concerned covert surveillance. It is common ground that the present case, in contrast, is concerned with overt surveillance.

65. Nor do we accept the Appellant's suggested analogy with the retention of fingerprints or DNA samples, which was considered by the European Court of Human Rights in *S v United Kingdom* (2009) 48 EHRR 50. Although that case is often cited (and was cited before us) in relation to the requirement that interference with Article 8 rights must be in accordance with the law, it should be noted that the European Court of Human Rights in fact declined to answer that question: see [95]-[99] of the judgment. This was because it considered that the questions raised in that context were closely related to the broader issue of whether the interference was necessary in a democratic society and, in view of its analysis of that issue at [105]-[126], it was not necessary to decide whether the wording of section 64 of the Police and Criminal Evidence Act 1984 was compatible with the "quality of law" requirements of Article 8(2).

66. When one turns to the Court's assessment of the proportionality issue in that case, it is clear, in our view, that its reasoning was heavily influenced by the particular sort of interference which was in issue. That case concerned the retention of fingerprints and DNA records. Furthermore, the legislation in issue permitted that retention even in the case of people such as the applicants who, having been arrested, had been acquitted and perhaps never even charged with an offence. The legislation permitted the blanket and indiscriminate retention of such personal data. There were no time limits and no restriction by reference to the type of offence. We consider, like the Divisional Court, that the context of that case is far removed from that of the present case.

67. On behalf of the Appellant Mr Squires also placed reliance on the judgment of Lord Reed JSC in *R (T) v Chief Constable of Greater Manchester and Others* [2014] UKSC 35, [2015] AC 49, at [114], where he said:

> "… in order for the interference to be 'in accordance with the law', there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. Whether the interference in a given case was in fact proportionate is a separate question."

68. A similar point was made again by Lord Reed in *Christian Institute v Lord Advocate* [2016] UKSC 51; [2017] SC (UKSC) 29, at [80], where he cited his earlier judgment in *T*.

69. The short answer, in our view, to this submission is that the legal framework which regulates the deployment of AFR Locate *does* contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary.

70. Mr Squires also submitted, in reliance on *Christian Institute*, that it was not sufficient that it is possible for a court or tribunal to assess the question of proportionality after

the event, because a person whose Article 8 rights are interfered with may never know that the interference has taken place and should be put in a position where they are able to mount an effective challenge. It seems to us that the answer to that point is that, in the present context, as the Divisional Court found, SWP did all that could reasonably be done to bring to the public's attention that AFR Locate was being deployed at a particular place at a particular time. As is common ground, AFR Locate was deployed in an overt manner. In any event, *Christian Institute* was concerned with particular legislation of the Scottish Parliament: what was said in that case cannot be taken out of context as if it were a rule of general application set out in a statute.

71. We must now turn to the decision of the Supreme Court in *R (Catt) v Association of Chief Police Officers*. That decision formed the mainstay of the submissions for SWP and the Secretary of State, as well as the reasoning of the Divisional Court.

72. *Catt* concerned the collection, retention and use of personal data about an individual on a database whose existence was not acknowledged to exist until the judicial review proceedings in that case itself. The police maintained what was described as an "extremism database". The claimant had been a regular attender at peace movement demonstrations since 1948. In 2005 he began participating in demonstrations of an organisation called Smash EDO, a number of which involved serious disorder and criminality. The applicant was arrested twice but never convicted of any offence. When he made a request to the police under the DPA 1998, entries on the database concerning protests at which he had taken part were disclosed to him.

73. The database contained information about the claimant in the form of a single photograph, subsequently destroyed, and written references to him in a number of information reports on other people. In the majority of those reports all that was recorded about the claimant was the fact of his presence at a protest and his date of birth and address but some also described his appearance. The police undertook the collection of the data on the basis of general common law powers.

74. The retention and use of the data were regulated by the DPA 1998, by the 2005 Code of Practice on the Management of Police Information issued by the Secretary of State pursuant to section 39A of the Police Act 1996, and by the associated administrative guidance. That framework of legal regulation was held by the Supreme Court to be sufficient. The main judgment was given by Lord Sumption JSC (with whom Lord Neuberger PSC agreed).

75. At [1], Lord Sumption began his judgment with the following:

> "This appeal is concerned with the systematic *collection* and retention by police authorities of electronic data about individuals. The issue in both cases is whether the practice of the police governing retention is lawful …" (Emphasis added)

76. We therefore reject Mr Squires's submission that *Catt* was concerned only with the retention of information and not with its collection.

77. Lord Sumption went on to note, in the same paragraph, that a particular feature of the data in that case was that they consisted entirely of records made of acts of the applicant

which took place in public. The information had not been obtained by any intrusive technique such as bugging or DNA sampling. We accept that is a feature of the present case too.

78. At [7], Lord Sumption said that, at common law, the police have the power to obtain and store information for policing purposes, *i.e.* broadly speaking for the maintenance of public order and the prevention and detection of crime. Those powers do not authorise intrusive methods of obtaining information, such as entry on private property, but they were amply sufficient to authorise the obtaining and storage of the kind of public information in that case.

79. Lord Sumption considered the question of whether the interference in that case was in accordance with the law at [11]-[17]. He concluded that it was. He rejected the suggestion that the fact that the DPA was a statute of general application meant that it did not provide sufficient protection in the specific context of data obtained or stored by the police. As Lord Sumption said at [12]:

> "… It lays down principles which are germane and directly applicable to police information, and contains a framework for their enforcement on the police among others through the Information Commissioner and the courts."

80. Lord Sumption rejected the argument advanced on behalf of the appellant in that case that he was entitled to know precisely what data would be obtained and stored or for how long. He said that that was not realistic. "The infinite variety of situations in which issues of compliance may arise and the inevitable element of judgement involved in assessing them make complete codification impossible." (See [14] and to similar effect [11]). Lord Sumption said that what is required is law which is "reasonably predictable, if necessary with the assistance of expert advice" but, except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. "It is enough that it lays down principles which are capable of being predictably applied to any situation."

81. For the sake of completeness, it should be noted that, when the case of *Catt* went to the European Court of Human Rights, that Court found there to be a violation of Article 8 on the ground that the interference with the applicant's right to respect for private life was disproportionate: see *Catt v United Kingdom* (2019) 69 EHRR 7, at [128]. The Court concluded that the question of whether the interference was in accordance with the law was in that case closely related to the broader issue of whether it was necessary in a democratic society and, in view of its analysis on that question, the Court did not find it necessary to decide whether the interference was in accordance with the law: see [106]-[107].

82. Mr Beer QC urged upon us, on behalf of SWP, what he described as a "relativist approach". He cited the judgment (in part dissenting) of Laws LJ in *R (Wood) v Metropolitan Police Commissioner* [2009] EWCA Civ 414, [2009] 4 All ER 951, at [53], where he said:

> "There is some suggestion in the cases of a relativist approach, so that the more intrusive the act complained of, the more precise and specific must be the law said to justify it."

83. In his submissions in reply Mr Squires confirmed that he would accept the "relativist" approach. We too would be prepared to accept that as a matter of principle. The crucial question, as it seems to us, is the application of that principle to the particular context.

84. We are conscious that the police have long used techniques to gather information which are undoubtedly in accordance with the law. For example, they have the power to observe what they see in a public place, to record that information and to retain it in their files. Just as the human eye can observe a person in a public place, so the police have the power to take photographs of people.

85. We do not, however, accept the submission on behalf of SWP that the present context is analogous to the taking of photographs or the use of CCTV cameras. The following features of the present case lead us to conclude that it falls somewhere in between the two poles on a spectrum which are represented by *S v UK* on the one hand and *Catt* on the other.

86. First, AFR is a novel technology.

87. Secondly, it involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police.

88. Thirdly, it is acknowledged by all concerned that this is "sensitive" personal data, within the meaning of the DPA 2018. That Act in turn reflects EU legislation. This represents an institutional recognition of the sensitivity of the data concerned, a feature which is not present for example for ordinary photographs.

89. Fourthly, the data is processed in an automated way.

90. We accept a large part of the analysis of the Divisional Court but not all of it. We consider that the legal framework which the Divisional Court regarded as being sufficient to constitute the "law" for the purposes of Article 8(2) is on further analysis insufficient.

91. The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the "who question" at the hearing before us. The second is the "where question". In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed.

92. The DPA 2018 and the relevant policies in substance require only that there has to be a proper law enforcement purpose. The use of the measure must then be considered to be necessary to achieve that purpose.

93. We would also emphasise that one of the elements of the system as operated in South Wales which is crucial, in our view, is that the data of anyone where there is no match

with a person on the watchlist is automatically deleted without any human observation at all and that this takes place almost instantaneously. We would hope that that feature of the current scheme would not simply be set out in a policy document by way of description but that it would be made clear that such automatic and almost instantaneous deletion is required for there to be an adequate legal framework for the use of AFR Locate.

94. We would accept, and indeed it was common ground, that it is not for the Appellant or for this Court to design a particular set of policies in order for them to comply with the quality of law requirement. We are satisfied, however, that the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law.

95. We make it clear that we would not wish to be unduly prescriptive as to the content of any new policies, for example the principle of "neither confirm nor deny" is well-established and would have to be respected.

96. It might even be that, once the "who" question can be satisfactorily resolved, that will give clear guidance as to the "where" question. This is because it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watchlist are going to be at that location.

97. We now turn in more detail to each of the three elements of the legal framework which the Divisional Court found to be sufficient to have the quality of law in the present context: the DPA 2018, the Surveillance Camera Code of Practice and SWP's local policies.

Data Protection Act 2018

98. As Mr Beer pointed out at the hearing before us, the present context is governed not simply by the general provisions in the DPA 2018 but by Part 3, which deals specifically with the subject of law enforcement processing.

99. Section 31 defines "the law enforcement purposes" in this context as:

> "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."

100. Chapter 2 of Part 3 sets out the governing principles. Section 34 provides an overview and explains that the Chapter sets out the six data protection principles. The first data protection principle, set out in section 35(1), is that processing must be lawful and fair.

101. Amongst the requirements of the first data protection principle, set out in section 35, are the following. 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: see subsection (2).

102. In addition, where the processing is "sensitive processing", it is permitted only in the two cases set out in subsections (4) and (5). Of particular relevance in the present context is subsection (5), which deals with the situation 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 in accordance with section 42.

103. Schedule 8, which sets out conditions for sensitive processing under Part 3, provides that the condition in paragraph 1 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."

104. We accept, as did the Divisional Court, that the legal protections in the DPA 2018 form an important part of the framework in determining whether the interference with the Appellant's Article 8 rights was in accordance with the law. That Act is not, however, sufficient by itself, nor was it suggested that it is.

105. Before leaving the DPA 2018 we should mention one further matter. In the skeleton argument on behalf of the Information Commissioner it was submitted that the Divisional Court had fallen into error by putting the cart before the horse in that it had addressed the question of the requirement of law in Article 8(2) of the Convention before considering whether there had been compliance with section 35 of the DPA 2018. In particular, it was submitted that the processing of the data in the present case was not "based on law" within the meaning of section 35(2) of the DPA 2018, interpreted in accordance with the EU's Law Enforcement Directive and the Convention, because there was no legal basis for the processing that was clear, precise and foreseeable in its application. It was also submitted that the processing was not "strictly necessary" for the law enforcement purposes as required by section 35(5)(a) of the DPA 2018.

106. Since, it was submitted, there was a breach of section 35(2), there could not be "accordance with the law" for the purpose of Article 8(2). Detailed submissions were made as to the requirements of strict necessity, citing authority from both the Court of Justice of the European Union and the Supreme Court of the UK.

107. At the hearing before us we made it clear that we did not regard these submissions as properly falling within the scope of the present appeal. The submissions were made by an intervener in the context of Ground 1 in the appeal. Ground 1 was formulated as follows on behalf of the Appellant:

> "The Divisional Court erred in concluding that the interference with the Appellant's rights under Article 8(1) … occasioned by the Respondent's use of live automated facial recognition technology … on 21 December 2017 and 27 March 2018 and on an ongoing basis was/is in accordance with the law for the purposes of Article 8(2) ECHR."

108. It is clear therefore that the submissions advanced on behalf of the Information Commissioner, at least in writing, went beyond the scope of Ground 1 since they

focused on the requirements of domestic legislation, namely section 35 of the DPA 2018.

The Surveillance Camera Code of Practice

109. Section 29 of the PFA 2012 imposes a duty on the Secretary of State to prepare a Code of Practice containing guidance about surveillance camera systems. The section goes on to prescribe what the Code must contain and what it may include provision about. The term "surveillance camera systems" is defined in subsection (6) to mean:

> "(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), or
>
> (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a) (b) or (c)."

110. It was common ground that AFR falls within that definition.

111. Under section 30 of the PFA 2012 the Secretary of State must lay a draft of an order providing for the Code to come into force, and the Code itself, before Parliament. She must then make the order and issue the Code if the draft is approved by resolution of each House of Parliament. Such an order is to be in the form of a statutory instrument.

112. The effect of the Code is governed by section 33 of the PFA 2012. A relevant authority must have regard to the Code when exercising any functions to which the Code relates: see subsection (1). A relevant authority includes for this purpose any chief officer of a police force in England and Wales: see subsection (5)(j). A failure on the part of any person to act in accordance with any provision of the Code does not of itself make that person liable to criminal or civil proceedings: see subsection (2). The Code is admissible in evidence in any such proceedings: see subsection (3). In particular, a court or tribunal may take into account a failure by a relevant authority to have regard to the Code: see subsection (4).

113. Under section 34 of the PFA 2012 the Secretary of State must appoint a person as the Surveillance Camera Commissioner. The Commissioner has the following functions: (a) encouraging compliance with the Code, (b) reviewing the operation of the Code, and (c) providing advice about the Code (including changes to it or breaches of it). It is common ground that the Commissioner does not have powers of enforcement, although the Information Commissioner does.

114. The Surveillance Camera Code of Practice was issued by the Secretary of State for the Home Department in June 2013, under section 30 of the PFA 2012. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities, including for this purpose the police. It is general in its scope and

is not specifically concerned with facial recognition technology, although that topic is referred to in the Code. The Code sets out 12 guiding principles at para. 2.6. By way of example the first guiding principle is that:

> "Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need."

115. Para. 3.2.3 specifically addresses the subject of facial recognition in the following way:

> "Any 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."

116. Para. 4.12.1 states:

> "Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose."

117. Para. 4.12.2 states:

> "A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database."

118. In the light of the fact that the Code does deal specifically with such matters, it seems to us that it could in principle also deal specifically with what the requirements are for inclusion on a police force's watchlist. It could also deal with what policies should contain in relation to the location of the deployment of AFR Locate. As we have said earlier, the question whether such policies must be set out in a national document such as this Code or whether they should be set out in local policies determined by each police force is not a matter for this Court. It may be prudent, however, for there to be at least consistency in the content of local policies and that might be the appropriate subject of an amendment to the Code by the Secretary of State.

119. Our attention was also drawn to the guidance which has been published by the Surveillance Camera Commissioner (March 2019) on 'The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems'.

120. The guidance does address the question of images of persons on a watchlist at paras. 14.1-14.3. We note, however, that the guidance does not contain any requirements as to the content of local police policies as to who can be put on a watchlist. Nor does it contain any guidance as to what local policies should contain as to where AFR can be deployed. Those, as we have said, are the two critical defects in the current legal framework.

SWP's local policies

121. As we have said, in principle a police force's local policies can constitute relevant "law" in the present context, provided they are published. The critical question, in our view, is how much discretion the policies in this case leave to the police, particularly in relation to the question who can be put on a watchlist and the question of the location where AFR Locate can be deployed.

122. When asked about these questions at the hearing Mr Beer helpfully drew our attention to a number of documents.

123. First, Mr Beer referred to the Privacy Impact Assessment produced by SWP. At para. 1.9, in addressing the question whether there is a specific business purpose that requires the use of the information, the answer included the following in relation to those on the watchlist:

> "These individuals could be persons wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence is required."

124. While we can readily understand that the first three of those categories are objective, the final category is not. In effect it could cover anyone who is of interest to the police. In our judgement, that leaves too broad a discretion vested in the individual police officer to decide who should go onto the watchlist.

125. Matters are not assisted by the fact that the next document to which our attention was drawn, the DPIA produced under the DPA 2018, does not include that last category (of intelligence purposes) at all. That document (at page 5) says that the purpose of AFR is to identify and locate:

(1) Individuals suspected of criminality and who are wanted by the courts and police.

(2) Individuals who may pose a risk to themselves and others.

(3) Individuals who may be vulnerable.

126. Mr Beer also drew our attention to what is set out in page 16 of that same document. That, however, seems to us not to be material in the present appeal, since that concerns the application of the Regulation of Investigatory Powers Act 2000. As is common ground, covert surveillance is governed by that legislation and would require authority under the system of warrants created by that Act. Overt surveillance, in contrast, such as AFR Locate (as it was carried out by SWP on the facts of the present case) does not require such authorisation.

127. Mr Beer also drew our attention to what is said at page 20 of the same document:

> "Concerns have been raised by privacy experts that an individual may seek to enquire as to whether they have been included in a watchlist outside of the 24-hours retention period. Therefore, it has been deemed appropriate to be able to re-engineer watchlists. This can now be achieved via Niche RMS 'back-end' database by recording the nominal number of an individual extracted into a watchlist for on given date, this added functionality is available from October 2018."

With respect, it seems to us that deals with a technical matter and does not govern the question of who can be properly placed on a watchlist.

128. Finally, in the context of who can be placed on a watchlist Mr Beer drew our attention to SWP's Standard Operating Procedure, at page 6, where it is said:

> "3. AFR Locate
>
> The system works by means of a pre-populated **Watch List** which will contain information and images of subjects and a pre-defined response should these subjects be located by the system.
>
> Watchlists will be both proportionate and necessary for each deployment with the rationale for inclusion detailed pre-event in the AFR Locate deployment report.
>
> Primary factors for consideration for inclusion within a watchlist will be watchlist size, image quality, image provenance and rationale for inclusion.
>
> The numbers of images included within a watchlist cannot exceed 2,000 due to contract restrictions but in any event 1 in 1000 false positive alert rate should not be exceeded.
>
> Children under the age of 18 will not ordinarily feature in a watchlist due the reduced accuracy of the system when considering immature faces.
>
> However, if there is a significant risk of harm to that individual a risk based approach will be adopted and rationale for inclusion evidenced within the deployment report.
>
> The decision for an AFR deployment wherever possible will ultimately be made by the Silver Commander with the DSD project team acting as tactical advisors. Wherever possible the deployment of AFR Locate should be detailed with the Silver Commanders Tactical plan.
>
> If a deployment does not feature a Silver Commander the rationale for deployment will be ratified by the Digital Services

> Division Inspector and be detailed within the AFR Locate Deployment Report."

129. Again, it seems to us, that does not govern the question of who can be put on a watchlist in the first place.

130. So far as the location of deployment is concerned, Mr Beer really was not able to draw our attention to anything which specifies where AFR Locate may be deployed. He drew our attention to the (unnumbered) paragraphs 7-9 and 11 of the Standard Operating Procedure, again at page 6 of that document. He also drew our attention to page 21 of the DPIA, where it is said:

> "As we are testing the technology South Wales Police have deployed in all event types ranging from high volume music and sporting events to indoor arenas."

That simply underlines the concern that we have in this context. First, it is a descriptive statement and does not lay down any normative requirement as to where deployment can properly take place. Secondly, the range is very broad and without apparent limits. It is not said, for example, that the location must be one at which it is thought on reasonable grounds that people on the watchlist will be present. These documents leave the question of the location simply to the discretion of individual police officers, even if they would have to be of a certain rank (a "Silver Commander"). For the above reasons this appeal will be allowed on Ground 1.

Ground 2: Proportionality

131. Strictly speaking, it is unnecessary for this Court to consider Ground 2 in this appeal, which relates to the question of proportionality, since, if (as we have held) the interference with the Appellant's Article 8 rights was not in accordance with the law, one never reaches the stage of asking whether that interference was proportionate. Nevertheless, as we heard full argument on Ground 2, we will address it.

132. The Divisional Court addressed the question of proportionality at [98]-[108]. It set out the relevant principles for the objective justification of a limitation on a Convention right at [98] by setting out four questions which are now very familiar:

> "If an interference with Article 8(1) rights is to be justified it must meet the four-part test in *Bank Mellat v Her Majesty's Treasury (No 2)* [2014] AC 700, namely:
>
> (1) whether the objective of 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 without unacceptably compromising the objective; 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.
>
> (See *per* Lord Sumption at [20]; and especially on question (3), *per* Lord Reed at [70] to [71] and [75] to [76]).”

133. As before the Divisional Court, so before this Court there is no dispute as regards the first two of those questions. Mr Squires did not make any submissions before us in relation to the third question either. What he did submit was that the Divisional Court fell into error in answering the fourth question, whether a fair balance has been struck between the rights of the individual and the interests of the community. The Court answered that question at [101] as follows:

> “Nevertheless, we are satisfied that the use of AFR Locate on 21st December 2017 (Queen's Street) and 27th March 2018 (Motorpoint Arena) struck a fair balance and was not disproportionate. AFR Locate was deployed in an open and transparent way, with significant public engagement. On each occasion, it was used for a limited time, and covered a limited footprint. It was deployed for the specific and limited purpose of seeking to identify particular individuals (not including the Claimant) who may have been in the area and whose presence was of justifiable interest to the police. On the former occasion it led to two arrests. On the latter occasion it identified a person who had made a bomb threat at the very same event the previous year and who had been subject to a (suspended) custodial sentence. On neither occasion did it lead to a disproportionate interference with anybody's Article 8 rights. Nobody was wrongly arrested. Nobody complained as to their treatment (save for the Claimant on a point of principle). Any interference with the Claimant's Article 8 rights would have been very limited. The interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant's biometric data. No personal information relating to the Claimant would have been available to any police officer, or to any human agent. No data would be retained. There was no attempt to identify the Claimant. He was not spoken to by any police officer.”

134. Mr Squires accepts that, on an appeal, it is not the function of this Court simply to make its own assessment of whether an interference with a Convention right was proportionate. The question for this Court is whether the assessment made by the Divisional Court was “wrong”, bearing in mind that this appeal consists of a review rather than a re-hearing. Mr Squires submits that the Divisional Court fell into error as a matter of approach when addressing the question of proportionality. He makes two main submissions on behalf of the Appellant.

135. First, he submits that the "benefit" side of the proportionality balance needs to take into account not only the *actual* results of an operation when AFR Locate is deployed but its *anticipated* benefits. Although that may well be right as a matter of principle, it seems to us that that is a point in favour of SWP rather than the Appellant. In any event, it does not seem to us that the Divisional Court fell into error in its approach in this way.

136. Secondly, Mr Squires submits that the Divisional Court erred when examining the "cost" side of the proportionality balance by taking into account only the impact of the AFR deployment on this particular Appellant. He submits that, as a matter of common sense, account needs to be taken of the interference with the Article 8 rights not only of this particular Appellant but all other members of the public who would have been at the two venues in question when AFR Locate was deployed on 21 December 2017 and 27 March 2018.

137. In support of that submission Mr Squires cited several dicta from the Supreme Court. In particular, he referred to *R (Tigere) v Secretary of State for Business, Innovation and Skills* [2015] UKSC 57, [2015] 1 WLR 3820, at [33], [39] and [41] in the judgment of Lady Hale DPSC. For example, at [39], Lady Hale referred to "the impact on the appellant and *others in her position*" (emphasis added). Conversely, earlier in the same paragraph, as Mr Beer pointed out to us, she referred to "the fair balance to be struck between the effect on *the person* whose rights have been infringed and the interests of the community" (emphasis added).

138. Mr Squires also cited the *Christian Institute* case, at para. 90, where the Court set out the familiar criteria for assessing proportionality and, under the fourth question, summarised it as being:

> "Whether, balancing the severity of the measure's effects on the rights of *the persons to whom it applies* against the importance of the objective, to the extent that the measure would contribute to its achievement, the former outweighs the latter (i.e. whether the impact of the rights infringement is disproportionate to the likely benefit of the impugned measure)." (Emphasis added)

139. It seems to us that the answer to a human rights question cannot depend on semantics, for example the use of the singular or the plural used by a judge in one passage in a judgment rather than in another passage. The issue has to be addressed as a matter of legal principle.

140. It may well be that in cases such as *Tigere*, where what is under challenge is a general measure, for example a policy or even a piece of legislation, it is appropriate for the Court to assess the balance between the impact on every person who is affected by the measure and the interests of the community. The present challenge, however, was not to such a general measure. The challenge was to a very specific deployment of AFR Locate on two particular occasions and the argument made in the Statement of Facts and Grounds was simply that this Appellant's Article 8 rights had been violated.

141. It is significant that, in the Statement of Facts and Grounds, at para. 2, the complaint brought by the Appellant was formulated in the following way:

> "… On at least two occasions, in December 2017 and March 2018, the Claimant was targeted by the Defendant's use of AFR. Through this claim he challenges:
>
> (i) the unlawful use of this technology *against him* on both occasions, and
>
> (ii) the Defendant's ongoing use of AFR in public places in the police area in which he resides, giving rise to a clear risk of the technology again being used *against him*." (Emphasis added)

142. It is clear therefore that the substance of the complaint being made by the Appellant in this claim for judicial review was the impact of the use of AFR by SWP against him, not anyone else. This point was developed at paras. 17-22 of the Statement of Facts and Grounds, which set out more detail about the events of 21 December 2017 and 27 March 2018. The point was summarised as follows at the beginning of para. 17:

> "It is the Claimant's case that he has twice been the subject of the Defendant's use of AFR technology …"

143. Further, and in any event, we accept the submission made by Mr Beer on behalf of SWP that the impact on each of the other members of the public who were in an analogous situation to this Appellant on the two occasions with which we are concerned for present purposes (in December 2017 and March 2018) was as negligible as the impact on the Appellant's Article 8 rights. An impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement.

144. For those reasons we would reject Ground 2.

Ground 3: Compliance with section 64 of the DPA 2018

145. This ground of appeal is limited to two alleged deficiencies in the DPIA. The first is that there was a material error of law "concerning the non-engagement of Article 8" of the Convention. The second is that there was a material error of law concerning "the processing of the (biometric) personal data of persons whose facial biometrics are captured by AFR but who are not on police watch lists used for AFR".

146. Mr Squires made no oral submissions on this ground of appeal and relied upon his skeleton argument. Mr Facenna both relied on his skeleton argument and advanced oral submissions in support of this ground of appeal.

147. Three criticisms of the DPIA are made in Mr Squires's skeleton argument. First, the DPIA's analysis of the application of data protection principles contained no recognition that AFR entails the processing of the personal data (and still less the biometric data) of persons not on watchlists. Second, the DPIA did not acknowledge that the Article 8 rights of such persons are engaged. Third, the DPIA was silent as to the risks to other rights which are likely to be affected by the use of AFR: the rights to

freedom of assembly under Article 11 of the Convention and freedom of expression under Article 10 of the Convention. There is no further elaboration of those points. The skeleton argument concludes, on this ground of appeal, that in the light of those three alleged deficiencies, the DPIA fell foul of the test specified by the Divisional Court itself (at [146]), namely:

> "If it is apparent that a data controller has approached its task on a footing that is demonstrably false, or in a manner that is clearly lacking, then the conclusion should be that there has been a failure to meet the section 64 obligation".

148. Mr Facenna's skeleton argument made the following criticisms of the DPIA. First, the DPIA contained no assessment of the impact of the deployment of AFR on the protection of the personal data of members of the public who might be affected by the measures. Secondly, it contained no assessment of the risks to their rights and freedoms, so that, for example, there was little or no engagement with the fact that SWP's use of AFR involved the collection of data on a blanket and indiscriminate basis, and it placed too little weight on the interference posed by the initial collection itself and the plainly ambitious scale of the collection, particularly bearing in mind that it involved the sensitive processing of biometric data. Thirdly, the assessment did not adequately address the risk that a false positive would result in innocent members of the public having their biometric data retained for longer periods and place them at risk of being subjected to more intrusive interventions by police. Fourthly, the assessment of the right to privacy under Article 8 of the Convention, privacy risks, and possible mitigation of those risks, was negligible at best, being more concerned with the technical operation of AFR.

149. In his oral submissions Mr Facenna said that the DPIA did not contain an assessment of privacy, personal data and safeguards. He said it contained no acknowledgment that AFR involves the collection of data on a blanket and indiscriminate basis and that the risk of false positives would mean a longer period of retention. He criticised the DPIA for failing to address the potential for gender and racial bias. Generally, he submitted that there was a failure in the DPIA to provide an assessment of the risks and mitigation of them, as required by section 64 of the DPA 2018. He said that the Divisional Court's dismissal of the claim under section 64 has to be seen in the context of the conclusion of the Divisional Court that Article 8 was not infringed for non-matched members of the public.

150. Some of the criticisms now advanced by the Appellant and the Information Commissioner in respect of the DPIA fall outside the alleged two material errors of law specified in this ground of appeal. They include the point in Mr Squires's skeleton argument that the DPIA does not refer to interference with the Convention rights to freedom of assembly and expression (Articles 10 and 11) and Mr Facenna's arguments that a false positive would result in innocent members of the public having their biometric data retained for longer periods and place them at risk of being subjected to more intrusive interventions by police and that the DPIA failed to address the potential for gender and racial bias.

151. We agree with the Divisional Court that some of the criticisms of the DPIA made by Mr Squires and Mr Facenna are unjustified. The DPIA specifically acknowledged that

AFR might be perceived as being privacy intrusive in the use of biometrics and facial recognition and that Article 8 of the Convention was relevant. It sought to explain that AFR would only avoid being in breach of Article 8 if it was necessary, proportionate, in pursuit of a legitimate aim and in accordance with the law but that all those requirements would be satisfied if AFR Locate was used in the manner set out. The DPIA explained how AFR Locate operates. It is obvious from that explanation that large numbers of the public would be caught through CCTV cameras used in the deployment. It specifically stated that: "It is the intention during each deployment to allow the AFR application to enrol and therefore process as many individuals as possible". That the public at large was potentially affected was reflected in the statement that: "in order to ensure that the public are engaged in the use of the technology every opportunity has been taken to demonstrate its use, to include during Automated Facial Recognition deployments".

152. This Ground of Appeal is, however, correct insofar as it states that the DPIA proceeds on the basis that Article 8 is not engaged or, more accurately, is not infringed. We have found, when considering Ground 1 above, that AFR Locate fails to satisfy the requirements of Article 8(2), and in particular the "in accordance with the law" requirement, because it involves two impermissibly wide areas of discretion: the selection of those on watchlists, especially the "persons where intelligence is required" category, and the locations where AFR may be deployed.

153. The inevitable consequence of those deficiencies is that, notwithstanding the attempt of the DPIA to grapple with the Article 8 issues, the DPIA failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found, as required by section 64(3)(b) and (c) of the DPA 2018.

154. For those reasons, we will allow the appeal on this ground.

Ground 4: Compliance with section 42 of the DPA 2018

155. The Appellant submits that one of the reasons why the use of AFR involves the unlawful processing of personal data is because SWP has failed to satisfy the requirements of the first data protection principle in section 35 of the DPA 2018. The Divisional Court held that the processing was for law enforcement purposes and was sensitive processing within section 35(3). In the circumstances of the present case, this meant that the processing had to satisfy the requirements in section 35(5), which included (in section 35(5)(c)) that, "at the time when the processing is carried out, the controller has an appropriate policy document in place". Section 42 of the DPA 2018 sets out what such a document must contain.

156. As stated earlier, before the Divisional Court SWP relied on the November 2018 Policy Document. The Divisional Court thought that it was open to question whether that document, as then drafted, fully met the standard required by section 42(2) and said that ideally it should be more detailed. In paragraph [141] of their judgment, which we have quoted in full above, the Divisional Court said that the development and specific content of the document was, for the time being, better left for reconsideration by SWP in the light of further guidance from the Information Commissioner.

157. The Appellant's criticism is that the Divisional Court was obliged to reach a finding on whether the November 2018 Policy Document complied with section 42, and ought to have found that it did not.

158. We would reject this ground of appeal for reasons which can be shortly stated.

159. The two specific deployments which are the subject of the Appellant's claim took place on 21 December 2017 (Queen Street) and 27 March 2018 (Motorpoint Arena). Those were before the DPA 2018 came into force. There is no alleged failure to comply with the DPA 1998 on this point.

160. Accordingly, the only relevance of compliance with section 42 was in relation to any future use of AFR in which the Appellant's image might be captured and processed by AFR. A section 42 document is an evolving document, which, in accordance with section 42(3), must be kept under review and updated from time to time. At the time of the hearing before the Divisional Court no guidance had been issued by the Information Commissioner as to the contents of a section 42 document. The Divisional Court said (at [140]) that it would be desirable to see specific guidance from the Information Commissioner, in exercise of her powers under Schedule 13 to the DPA 2018, on what is required to meet the section 42 obligation. The Information Commissioner herself expressed the view to the Divisional Court that the November 2018 Policy Document contained sufficient information to comply with the requirements of section 42(2), if barely so. That view has been repeated by the Information Commissioner on this appeal. In the event, on 4 November 2019, after the Divisional Court's judgment, the Information Commissioner did publish guidance on what a section 42 document should contain – "Law Enforcement Processing: Part 3 Appropriate Policy Document Template". SWP have now revised their November 2018 Policy Document in the light of that guidance.

161. In those circumstances - particularly as the Information Commissioner had expressed the view to the Divisional Court that the November 2018 Policy Document satisfied section 42(2) but ideally should be more detailed and the Divisional Court itself was uncertain whether or not it did meet the standard required by section 42 - it was entirely appropriate for the Divisional Court to make no final judgment on the point and to leave the SWP to make such revisions as might be appropriate in the light of any future guidance by the Information Commissioner.

162. For those reasons we would reject this ground of appeal.

Ground 5: Public Sector Equality Duty

163. The terms of the PSED are set out in section 149(1) of the Equality Act 2010 as follows:

> "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;
>
> (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it."

164. The two protected characteristics that are relevant in the present case are race and sex. It is submitted on behalf of the Appellant that SWP are in breach of the PSED because they have never had due regard to the need to eliminate discrimination on those two grounds which may arise from the software which is used in the deployment of AFR Locate. It is said that there is scientific evidence that facial recognition software can be biased and create a greater risk of false identifications in the case of people from black, Asian and other minority ethnic ("BAME") backgrounds, and also in the case of women.

165. It is important to be clear that it is not alleged that the software used by SWP does have that effect. There is no claim brought on the basis of the negative obligations in the Equality Act, not to discriminate (whether directly or indirectly). Rather the complaint is based on an alleged breach of the positive duty to have due regard to the need to eliminate such discrimination.

166. As we have mentioned above, Ground 5 in this appeal was formulated as follows:

> "The Divisional Court was wrong to hold that the Respondent complied with the Public Sector Equality Duty in section 149 of the Equality Act 2010 in circumstances in which the Respondent's Equality Impact Assessment was obviously inadequate and based on an error of law (by failing to recognise the risk of indirect discrimination) and the Respondent's subsequent approach to assessing possible indirect discrimination arising from the use of AFR is flawed."

167. In the Appellant's skeleton argument for this appeal, at para. 47, the submission was maintained that the Equality Impact Assessment dated 13 April 2017 was erroneous in law because consideration was given only to the possibility that AFR might be *directly* discriminatory and no consideration was given to whether it might operate in an *indirectly* discriminatory manner. This argument was not pursued by Mr Squires at the hearing before us, although he did not formally abandon it. He made clear during the course of the hearing, when pressed by the Court, that his focus was on the alleged *continuing* failure to discharge the PSED, and not upon the Equality Impact Assessment of April 2017.

168. The Equality Impact Assessment of April 2017 was headed "Initial Assessment". The use of the word "initial" did not mean that the assessment was only provisional or that there would be a further or fuller assessment in due course. It meant only that the initial assessment had not led to any concerns which were thought to require further investigation. In any event, as is common ground, there has been no further Equality

Impact Assessment since April 2017. The focus of Mr Squires's submissions before us was on the point that the PSED is a continuing duty and, submits Mr Squires, there is a continuing breach of it.

169. This has always been part of the Appellant's case: see para. 92 of the Statement of Facts and Grounds, where it was made clear that the PSED is "an ongoing obligation."

170. The reasons of the Divisional Court for rejecting this ground of challenge were set out at [153]-[158] of its judgment.

171. At [153] the Divisional Court said:

> "In our view, on the facts of this case there is an air of unreality about the Claimant's contention. There is no suggestion that as at April 2017 when the AFR Locate trial commenced, SWP either recognised or ought to have recognised that the software it had licensed might operate in a way that was indirectly discriminatory. Indeed, even now there is no firm evidence that the software does produce results that suggest indirect discrimination. Rather, the Claimant's case rests on what is said by Dr Anil Jain, an expert witness. In his first statement dated 30th September 2018, Dr Jain commented to the effect that the accuracy of AFR systems generally could depend on the dataset used to 'train' the system. He did not, however, make any specific comment about the dataset used by SWP or about the accuracy of the NeoFace Watch software that SWP has licensed. Dr Jain went no further than to say that if SWP did not know the contents of the dataset used to train its system 'it would be difficult for SWP to confirm whether the technology is in fact biased'. The opposite is, of course, also true."

172. At [156]-[158] the Divisional Court said the following:

> "156. Thus, SWP may now, in light of the investigation undertaken to date by Mr. Edgell, wish to consider whether further investigation should be done into whether the NeoFace Watch software may produce discriminatory impacts. When deciding whether or not this is necessary it will be appropriate for SWP to take account that whenever AFR Locate is used there is an important failsafe: no step is taken against any member of the public unless an officer (the systems operator) has reviewed the potential match generated by the software and reached his own opinion that there is a match between the member of the public and the watchlist face.
>
> 157. Yet this possibility of future action does not make good the argument that to date, SWP has failed to comply with the duty under section 149(1) of the Equality Act 2010. Our conclusion is that SWP did have the due regard required when in April 2017 it commenced the trial of AFR Locate. At that time,

> there was no specific reason why it ought to have been assumed it was possible that the NeoFace Watch software produced more or less reliable results depending on whether the face was male or female, or white or minority ethnic. As we have explained, even now there is no particular reason to make any such assumption. We note that although Dr Jain states that 'bias has been found to be a feature of common AFR systems' he does not provide an opinion on whether, or the extent to which, such bias can be addressed by the fail-safe, such as ensuring that a human operator checks whether there is in fact a match.
>
> 158. In our view, the April 2017 Equality Impact Assessment document demonstrates that due regard was had by SWP to the section 149(1) criteria. The Claimant's contention that SWP did not go far enough in that it did not seek to equip itself with information on possible or potential disparate impacts, based on the information reasonably available at that time, is mere speculation. In any event, as matters had developed in the course of the trial since April 2017, it is apparent from Mr. Edgell's evidence that SWP continues to review events against the section 149(1) criteria. This is the approach required by the public-sector equality duty in the context of a trial process. For these reasons, the claim made by reference to section 149(1) of the Equality Act 2010 fails."

173. With respect to the Divisional Court, we do not consider that there is "an air of unreality" about the Appellant's contention that there has been a breach of the PSED. On the contrary, it seems to us to raise a serious issue of public concern, which ought to be considered properly by SWP.

174. The Divisional Court did not refer to any authority on the PSED, perhaps because the relevant legal principles were not in dispute. In any event, those principles were set out by McCombe LJ in *R (Bracking) v Secretary of State for Work and Pensions* [2013] EWCA Civ 1345, [2014] Eq LR 60, at [26]. It is unnecessary to set out that passage in full here. It is well known and has frequently been cited with approval since, including in *Hotak v Southwark LBC* [2015] UKSC 30, [2016] AC 811, at [73] (Lord Neuberger PSC).

175. In that summary McCombe LJ referred to earlier important decisions, including those of the Divisional Court in *R (Brown) v Secretary of State for Work and Pensions* [2008] EWHC 3158 (Admin); [2009] PTSR 1506, in which the judgment was given by Aikens LJ; and *R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills* [2012] EWHC 201 (Admin); [2012] HRLR 13, in which the judgment was given by Elias LJ. For present purposes we would emphasise the following principles, which were set out in McCombe LJ's summary in *Bracking* and are supported by the earlier authorities:

(1) The PSED must be fulfilled before and at the time when a particular policy is being considered.

(2) The duty must be exercised in substance, with rigour, and with an open mind. It is not a question of ticking boxes.

(3) The duty is non-delegable.

(4) The duty is a continuing one.

(5) If the relevant material is not available, there will be a duty to acquire it and this will frequently mean that some further consultation with appropriate groups is required.

(6) Provided the court is satisfied that there has been a rigorous consideration of the duty, so that there is a proper appreciation of the potential impact of the decision on equality objectives and the desirability of promoting them, then it is for the decision-maker to decide how much weight should be given to the various factors informing the decision.

176. We accept (as is common ground) that the PSED is a duty of process and not outcome. That does not, however, diminish its importance. Public law is often concerned with the process by which a decision is taken and not with the substance of that decision. This is for at least two reasons. First, good processes are more likely to lead to better informed, and therefore better, decisions. Secondly, whatever the outcome, good processes help to make public authorities accountable to the public. We would add, in the particular context of the PSED, that the duty helps to reassure members of the public, whatever their race or sex, that their interests have been properly taken into account before policies are formulated or brought into effect.

177. This is reinforced by the background to the enactment of the PSED. That background is to be found in the Stephen Lawrence Inquiry Report in 1999, which led to the Race Relations (Amendment) Act 2000. That Act introduced a new section 71 into the Race Relations Act 1976, to replace an earlier version which had applied only to local authorities. The provision has since been expanded to embrace other protected characteristics and now finds its place in section 149 of the Equality Act 2010.

178. The background is explained by Karon Monaghan QC in Equality Law (2nd ed., 2013), at para. 16.06:

> "The first of the modern equality duties was found again in section 71 of the RRA, but following amendments made to it by the Race Relations (Amendment) Act 2000 (enacting the General Race Equality Duty). The General Race Equality Duty in the amended section 71 of the RRA required that listed public authorities had 'due regard' to the need 'to eliminate unlawful racial discrimination' and 'to promote equality of opportunity and good relations between persons of different racial groups'. The Race Relations (Amendment) Act 2000 and the General Race Equality Duty within it were enacted to give effect to the recommendations in the Stephen Lawrence Inquiry Report and the Inquiry's findings of 'institutional racism'. The purpose of the General Race Equality Duty was to create a strong, effective,

> and enforceable legal obligation which placed race equality at the heart of the public authority's decision making. The new duty was intended to mark a major change in the law. It represented a move from a fault-based scheme where legal liability rested only with those who could be shown to have committed one or other of the unlawful acts. Instead, the duty-bearer, the public authority, was to be required to *proactively* consider altering its practices and structures to meet this statutory duty. This was considered important in light of the findings of the Stephen Lawrence Inquiry." (Emphasis added)

179. Public concern about the relationship between the police and BAME communities has not diminished in the years since the Stephen Lawrence Inquiry Report. The reason why the PSED is so important is that it requires a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population.

180. The importance of the PSED was emphasised in *R (Elias) v Secretary of State for Defence* [2006] EWCA Civ 1293, [2006] 1 WLR 3213, at [274], where Arden LJ (as she then was) said:

> "It is the clear purpose of section 71 [the predecessor to section 149] to require public bodies … to give advance consideration to issues of race discrimination before making any policy decision that may be affected by them. This is a salutary requirement, and this provision must be seen as an integral and important part of the mechanisms for ensuring the fulfilment of the aims of anti-discrimination legislation. …"

181. We acknowledge that what is required by the PSED is dependent on the context and does not require the impossible. It requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex.

182. We also acknowledge that, as the Divisional Court found, there was no evidence before it that there is any reason to think that the particular AFR technology used in this case did have any bias on racial or gender grounds. That, however, it seems to us, was to put the cart before the horse. The whole purpose of the positive duty (as opposed to the negative duties in the Equality Act 2010) is to ensure that a public authority does not inadvertently overlook information which it should take into account.

183. Against that background of principle we turn to examine the reasons given by the Divisional Court for rejecting this ground of challenge. There are two aspects of the present case which particularly impressed the Divisional Court.

184. The first was the fact that there is a "human failsafe" component in the way in which AFR Locate is used. This means that a positive match made by the automated system will never by itself lead to human intervention. Before such an intervention (for example a stop of a member of the public for a conversation with a police officer) can

take place, there must be two human beings, including at least one police officer, who have decided to act on the positive match.

185. We do not consider the "human failsafe" is sufficient to discharge the PSED. As a matter of principle, it is not material to the PSED, which as we have observed, is a duty as to the process which needs to be followed, not what the substance of the decision should be. Secondly, as was acknowledged at the hearing before us, human beings can also make mistakes. This is particularly acknowledged in the context of identification. We would note the well-known warnings which need to be given to juries in criminal trials about how identification can be mistaken, in particular where a person has never seen the person being identified before: see *R v Turnbull* [1977] QB 224. Further, and in any event, this feature of the present case does not seem to us to go to the heart of the Appellant's complaint under Ground 5, which is that SWP have not obtained information for themselves about the possible bias which the software they use may have.

186. The second matter which impressed the Divisional Court was the witness statement of PC Dominic Edgell, who found that there was virtually no difference in the statistics as to race or gender. We have considered that evidence.

187. Mr Edgell reviewed the AFR Locate deployments from after the UEFA Champions League Final of 2017 through to June 2018. During those deployments 290 alerts were generated. 82 were true positives and 208 were false positives. He says that it is important to note that these statistics are only of the persons who have generated an alert. The identity of those who passed the camera without generating an alert is unknown.

188. 188 of the alerts were males (65%). Of the 188 male alerts, 64 (34%) were true positives and 124 (66%) were false positives. In relation to females, of 102 alerts, 18 (18%) were true positives and 84 (82%) were false positives. A number of the female false alerts were matched against primarily two individuals who the AFR software provider would refer to as a "lamb". A lamb is a person whose face has such generic features that may match much more frequently.

189. Mr Edgell also reviewed the ethnicity of those who were the subject of an alert. Of the true positives (82) 98% were "white north European". Of the false positives (208) 98.5% were "white north European".

190. Mr Edgell therefore concludes, at para. 26:

> "From my experience and the information available to me, I have seen no bias based on either gender or ethnicity. …"

191. In our view, this does not constitute a sufficient answer to the challenge based on the PSED. As Mr Squires submitted, Mr Edgell was dealing with a different set of statistics. He did not know, for obvious reasons, the racial or gender profiles of the total number of people who were captured by the AFR technology but whose data was then almost immediately deleted. In order to check the racial or gender bias in the technology, that information would have to be known. We accept Mr Beer's submission that it is impossible to have that information, precisely because a safeguard

in the present arrangements is that that data is deleted in the vast majority of cases. That does not mean, however, that the software may not have an inbuilt bias, which needs to be tested. In any event, with respect to Mr Edgell, he is not an expert who can deal with the technical aspects of the software in this context.

192. We should address another submission which was made to us by Mr Beer for SWP although it did not feature in the reasoning of the Divisional Court. This submission arises from the scientific evidence which has been filed in these proceedings.

193. When the claim for judicial review was first lodged, reliance was placed in the Statement of Facts and Grounds on the first witness statement of Dr Anil Jain, dated 30 September 2018. Dr Jain is a professor in the Department of Computer Science and Engineering at Michigan State University in the United States. In his first witness statement he explains that the performance of AFR technology is affected by a number of variables, including "training datasets": see para. 38(a). What this means is that the particular software which is used is "trained". At para. 47, Dr Jain says that the accuracy of an AFR system depends to a considerable extent on the training dataset. He goes on to say, at para. 48, that AFR systems can suffer from training "bias". At para. 49, he says that one cause of such training bias can be any imbalance in the demographic of subjects in the training datasets, resulting in the AFR system having a high false alarm rate or a high false reject rate for that particular demographic. At para. 51 Dr Jain states that it would appear that SWP were not aware of the dataset used to train the AFR system in this case. For that reason, he states, it would be difficult for SWP to confirm whether the technology is in fact biased. As a minimum for confirming whether an AFR system is biased, the database statistics, such as the number of males to females, and different races considered, would need to be known.

194. At the hearing before us Mr Beer placed particular reliance on a witness statement, filed in response to the first witness statement of Dr Jain, by Mr Paul Roberts, dated 23 November 2018. The first point to note about Mr Roberts' statement is that it was obtained in response to the challenge brought in the present proceedings; it was not obtained proactively by SWP in order to fulfil the PSED.

195. Mr Roberts was employed by NEC (UK) Ltd as Head of Products and Solutions for Facial Recognition and is now employed by Northgate Public Services (UK) Ltd as Head of Global Facial Recognition. Both companies are subsidiaries of NEC Corporation. One of the products of the business is the NeoFace Watch software with which the present case is concerned.

196. Mr Roberts makes the point in his witness statement that Dr Jain's report gave a generic description of generally available AFR software in the marketplace but is not a fully accurate description of NeoFace Watch. He states that the NeoFace algorithm is trained in laboratories and, on a typically annual basis, a new version of the algorithm is released containing improvements from, amongst other things, additional training. No further training is carried out by the system in any customer environments: see para. 10 of his witness statement. At para. 20, Mr Roberts states that the precise makeup, scale and sources of the training data used are commercially sensitive and cannot be released. He was, however, able to share certain facts, which he sets out in the following paragraphs. At para. 22 he states that:

> "To minimise any impact of bias as a result of gender, the NeoFace Algorithm training data set contains roughly equal quantities of male and female faces."

At para. 24 he states that the NeoFace Algorithm training data includes a wide spectrum of different ethnicities and has been collected from sources in regions of the world to ensure a comprehensive and representative mix. He states that great care, effort and cost is incurred by NEC, as a socially responsible major corporation, to ensure that this is the case.

197. Dr Jain responded to Mr Roberts' statement in a second witness statement dated 25 January 2019. He fairly acknowledges, at para. 15, that he cannot comment on whether AFR Locate has a discriminatory impact as he does not have access to the datasets on which the system is trained and therefore cannot analyse the biases in those datasets. He goes on to say, however, that bias has been found to be a feature of common AFR systems and that SWP themselves are not in a position to evaluate the discriminatory impact of AFR Locate.

198. At paras. 24-28, Dr Jain specifically responds to the witness statement of Mr Roberts. He expresses the opinion that what Mr Roberts says is not sufficient to be able to determine that the NeoFace algorithm is not biased towards a particular demographic group. To make this determination, he says, a thorough evaluation needs to be done of the demographic composition of the NeoFace algorithm training dataset. Dr Jain states at para. 28, without that information SWP are not able to assess whether the training dataset is biased or may be.

199. We acknowledge that it is not the role of this Court to adjudicate on the different points of view expressed by Mr Roberts and Dr Jain. That would not be appropriate in a claim for judicial review, still less on appeal. The fact remains, however, that SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex. There is evidence, in particular from Dr Jain, that programs for AFR can sometimes have such a bias. Dr Jain cannot comment on this particular software but that is because, for reasons of commercial confidentiality, the manufacturer is not prepared to divulge the details so that it could be tested. That may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty under section 149.

200. Finally, we would note that the Divisional Court placed emphasis on the fact that SWP continue to review events against the section 149(1) criteria. It said that this is the approach required by the PSED in the context of a trial process. With respect, we do not regard that proposition to be correct in law. The PSED does not differ according to whether something is a trial process or not. If anything, it could be said that, before or during the course of a trial, it is all the more important for a public authority to acquire relevant information in order to conform to the PSED and, in particular, to avoid indirect discrimination on racial or gender grounds.

201. In all the circumstances, therefore, we have reached the conclusion that SWP have not done all that they reasonably could to fulfil the PSED. We would hope that, as AFR is a novel and controversial technology, all police forces that intend to use it in the future

would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.

202. For the above reasons this appeal will be allowed on Ground 5.

Procedural matters

203. For the sake of completeness we mention briefly two procedural matters which were before us at the hearing of the appeal. They both relate to applications to refer to new material, which was not before the Divisional Court because it did not exist at that time. This Court has a discretion to permit such evidence under CPR 52.21(2). It is well-established that the discretion is to be exercised having regard to the criteria in *Ladd v Marshall* [1954] 1 WLR 1489: see *Terluk v Berezovsky* [2011] EWCA Civ 1534, at [31]-[32] (Laws LJ).

204. The first request (no formal application being thought to be necessary) was made on behalf of the Information Commissioner to refer to two documents which have been issued by her since the judgment of the Divisional Court. The first of those documents is 'The Use of Live Facial Recognition Technology by Law Enforcement in Public Places' (31 October 2019). The other document is an 'appropriate policy document' template in relation to law enforcement processing under Part 3 of the DPA 2018.

205. Mr Beer did not object to our looking at these documents in general terms, although he did object insofar as reference might be made to any matter of fact which was not before the Divisional Court. While we found the first document interesting, it did not affect our decision or our reasons in this appeal. We have considered the 'appropriate policy document' template in relation to Ground 4 for the reasons we set out in paras. 160 and 161 of this judgment, which reflect the decision of the Divisional Court in paras. [139]-[141] of their judgment.

206. The other procedural matter to be addressed is an application on behalf of the Surveillance Camera Commissioner to adduce fresh evidence in the form of a letter dated 4 December 2019 which was sent to the Secretary of State by, amongst others, the Surveillance Camera Commissioner. This was said to be relevant to an issue mentioned by the Divisional Court in its judgment, at [44], where reference was made to the fact that the Secretary of State has set up an Oversight and Advisory Board ("the Board"), comprising representatives from the police and other bodies, including the Surveillance Camera Commissioner, "to coordinate consideration of the use of facial imaging and AFR by law enforcement authorities." As we understand it, a disagreement has arisen since the judgment of the Divisional Court between the Surveillance Camera Commissioner and the Secretary of State as to the role performed by the Board.

207. On behalf of the Secretary of State objection was taken to the admissibility of this evidence by Mr O'Brien, although he was content that we should look at it on a contingent basis.

208. We need not take time over this procedural dispute. It seems to us that Mr O'Brien was right to submit that the setting up of the Board was at most a peripheral point, mentioned in passing in the Divisional Court's judgment. It does not seem to us to have had any

material impact on that Court's judgment: in particular, that Court made no reference to the existence of the Board in its reasoning on the issue of whether the interference with Article 8 rights was in accordance with the law. In any event, it does not affect this Court's conclusions or reasoning in this appeal. For that reason we refuse the application to adduce fresh evidence on behalf of the Surveillance Camera Commissioner.

Conclusion

209. For the reasons we have given this appeal will be allowed on Grounds 1, 3 and 5. We reject Grounds 2 and 4.

210. As to the appropriate remedy, we consider that declaratory relief to reflect the reasons why this appeal has succeeded will suffice. In the circumstances which have arisen, the parties agree that the only remedy which is required is a declaration but they have not been able to agree the precise terms of a declaration. Having considered the rival contentions, we have concluded that the declaration proposed by SWP more accurately reflects the judgment of this Court. We will grant a declaration in the following terms:

1) The Respondent's use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis, which engaged Article 8(1) of the European Convention on Human Rights, was not in accordance with the law for the purposes of Article 8(2).

2) As a consequence of the declaration set out in paragraph 1 above, in respect of the Respondent's ongoing use of Live Automated Facial Recognition technology, its Data Protection Impact Assessment did not comply with section 64(3)(b) and (c) of the Data Protection Act 2018.

3) The Respondent did not comply with the Public Sector Equality Duty in section 149 of the Equality Act 2010 prior to or in the course of its use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis.

ANNEX A
LEGAL FRAMEWORK

Legislation

Data Protection Act 1998 ("DPA 1998")

1. 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".

2. Section 1(1) of the DPA 1998 defined "data processing" 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].

3. Section 4(4) provided that it was:

> "… 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].

4. The data protection principles were set out in Schedule 1 to the DPA 1998:

(1) Principle 1 is that personal data shall be processed fairly and lawfully and, in particular, shall not be "processed" at all unless it is necessary for a relevant purpose (referred to in Schedule 2 below). In the case of the police, the relevant purposes are the administration of justice and the exercise of any other function of a public nature exercised in the public interest.

(2) Principle 2 is that personal data may be obtained only for lawful purposes and may not be further "processed" in a manner incompatible with those purposes.

(3) Principle 3 is that the data must be "adequate, relevant and not excessive" for the relevant purpose.

(4) Principle 4 is that data shall be accurate and, where necessary, kept up to date.

(5) Principle 5 is that the data may not be kept for longer than is necessary for those purposes.

(6) Principle 6 is that personal data shall be processed in accordance with the rights of data subjects under this Act.

(7) Principle 7 is that proper and proportionate technical and organisational measures must be taken against the unauthorised or unlawful "processing" of the data.

(8) Principle 8 is that personal data shall not be transferred outside the European Economic Area unless the country ensures an adequate level of protection.

5. Schedule 2 included the following conditions:

> "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."

6. 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 DPA 1998.

Protection of Freedoms Act 2012 ("PFA 2012")

7. Chapter I of Part 2 of the PFA 2012 makes provision for the "Regulation of CCTV and Other Surveillance Camera Technology". The relevant provisions of the PFA 2012 relate to the overt use of "surveillance camera systems" in public places by "relevant authorities" in England and Wales.

8. Section 29(1) mandates the Secretary of State to prepare a code of practice containing guidance about surveillance camera systems. Section 29(5) requires consultation with the National Police Chief's Council, the Information Commissioner, the Investigatory Powers Commissioner, the Surveillance Camera Commissioner, the Welsh Ministers and other persons the Secretary of State considers appropriate.

9. Section 29(6) provides that a surveillance camera system means:

> "(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), or

> (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).” (emphasis added)

10. A surveillance camera system which makes use of AFR therefore falls within this definition and is addressed within the Surveillance Camera Code of Practice.

11. Section 30 provides that the Secretary of State must lay the code of practice and order providing for the code to come into force before Parliament, and that such an order is to be a statutory instrument.

12. Section 31 provides that the Secretary of State must keep the code under review and may alter or replace it.

13. 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.

14. Section 33 further sets out the responsibility of a relevant authority as follows:

> “(1) A relevant authority must have regard to the surveillance camera code when exercising any functions to which the code relates.
>
> (2) A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings.
>
> (3) The surveillance camera code is admissible in evidence in any such proceedings.
>
> (4) A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings.” (emphasis added)

15. Section 33(5) provides the list of “relevant authorities” for the purposes of this part of the Act. Section 33(5)(j) sets out the inclusion of any chief officer of a police force in England and Wales. The Chief Constable of South Wales Police is therefore a relevant authority for the purposes of this Act.

16. Section 34 provides for the appointment of a Surveillance Camera Commissioner by the Secretary of State. The Surveillance Camera Commissioner is an arms-length body funded by, but independent of, the Home Office. His role is, *inter alia*, to ensure public confidence in surveillance systems. Section 34 provides that the Commissioner's functions include:

> “(a) Encouraging compliance with the surveillance camera code;
>
> (b) Reviewing the operation of the code; and

(c) Providing advice about the code (including changes to it or breaches of it)."

17. 17. The Secretary of State issued and published a code of practice pursuant to ss.30 and 32 of the PFA 2012 in June 2013 as the Surveillance Camera Code of Practice (see further below).

Data Protection Act 2018 ("DPA 2018")

18. 18. The DPA 2018 came into force on 25th May 2018.

19. 19. Section 29 of the DPA 2018 provides:

PART 3 LAW ENFORCEMENT PROCESSING

"29 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by a competent authority of personal data wholly or partly by automated means, and

(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies. …"

20. Section 34 of the DPA 2018 provides an overview of the six data protection principles and the duties of the data protection controller:

"34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter."

21. Section 35 of the DPA regulates "sensitive processing" and specifies the conditions that must be satisfied before it may take place. Section 35 provides as follows:

"35 The first data protection principle

(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).

(6) The Secretary of State may by regulations amend Schedule 8—

(a) by adding conditions;

(b) by omitting conditions added by regulations under paragraph (a).

(7) Regulations under subsection (6) are subject to the affirmative resolution procedure.

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

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

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

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation."

22. Section 35 reflects the language and scope of Article 10 of the Data Protection Law Enforcement Directive (2016/680/EU).

"*Article 10 Processing of special categories of personal data*

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only…"

Definitions

23. Section 3(2) of the DPA 2018 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".

24. Section 35(8) of the DPA 2018 defines "sensitive processing" as activities including:

> "…the processing of… biometric data… for the purpose of uniquely identifying an individual."

25. Section 205(1) of 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".

Conditions

26. Section 35(5) prescribes conditions which must be satisfied before the processing of biometric data for law enforcement purposes may be permitted. These conditions are threefold: (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) the controller has an appropriate policy document in place (see section 42).

27. The Schedule 8 conditions include:

> "1. 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.
>
> 2. Administration of justice
>
> This condition is met if the processing is necessary for the administration of justice.
>
> …
>
> 6. Legal claims

This condition is met if the processing-

> (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)…"

28. Section 42 contains requirements in respect of the "appropriate policy document" referred to in section 35(4), that must be in place:

> "**42 Safeguards: sensitive processing**
>
> (1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on… a condition specified in Schedule 8).
>
> (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, and
> >
> > (c) make it available to the Commissioner, on request, without charge.
>
> (4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—
>
> > (a) …which condition in Schedule 8 is relied on,

(b) how the processing satisfies section 35 (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5) In this section, "relevant period", in relation to sensitive processing …in reliance on a condition specified in Schedule 8, means a period which—

(a) begins when the controller starts to carry out the sensitive processing …in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing."

29. Section 64 of the DPA 2018 provides:

"**Data protection impact assessment**

(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."

Code and Guidance

Secretary of State's Surveillance Camera Code of Practice

30. The Surveillance Camera Code of Practice ("SC Code") was issued by the Secretary of State in June 2013. There is a statutory obligation to have regard to that code when exercising any functions to which the code relates (see s.33 of the PFA 2012 above). The SC Code lays down a series of 12 "Guiding Principles" for the operators of surveillance camera systems. They are as follows:

> "1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
>
> 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.
>
> 3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
>
> 4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
>
> 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.
>
> 6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
>
> 7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
>
> 8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
>
> 9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

> 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.
>
> 11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
>
> 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."

31. The SC Code concerns "conventional" CCTV systems, but specifically addresses the use of AFR as part of a surveillance camera system (see paragraph 3.2.3 below). The SC Code also covers the broader spectrum of statutory and procedural considerations which apply to surveillance camera operators, including Human Rights, Data Protection, Investigatory Powers and the forensic integrity of images.

32. Relevant paragraphs from the SC Code are as follows (with emphasis added):

> "1.8 <u>This code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places.</u>"
>
> "2.1 Modern and forever advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images and information. This technology can be a valuable tool in the management of public safety and security, in the protection of people and property, in the prevention and investigation of crime, and in bringing crimes to justice. Technological advances can also provide greater opportunity to safeguard privacy. Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need."
>
> "2.2 In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with the right provided that the interference is in pursuit of a legitimate aim and the interference is proportionate. Amongst the qualified rights is a person's right to respect for their private and family

life, home and correspondence, as provided for by Article 8 of the ECHR."

"2.3 That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential, now and in the future. In considering the potential to interfere with the right to privacy, it is important to take account of the fact that expectations of privacy are both varying and subjective. In general terms, one of the variables is situational, and in a public place there is a zone of interaction with others which may fall within the scope of private life. An individual can expect to be the subject of surveillance in a public place as CCTV, for example, is a familiar feature in places that the public frequent. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place."

"2.4 The decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented as the stated purpose for any deployment. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. Decisions over the most appropriate technology should always take into account its potential to meet the stated purpose without unnecessary interference with the right to privacy and family life. Furthermore, any deployment should not continue for longer than necessary."

"3.2.3 Any 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[4]. It should always involve human intervention before decisions are taken that affect an individual adversely." (Footnote 4: "The Surveillance Camera Commissioner will be a source of advice on validation of such systems.")

"4.8.1 Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body-worn video recorders."

"4.12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by

> others should not be introduced without regular assessment to ensure the underlying data is fit for purpose."
>
> "4.12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on a reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database."

Surveillance Camera Commissioner's AFR Guidance

33. The Surveillance Camera Commissioner has published "guidance" or "advice" on the use of AFR by the police in conjunction with CCTV entitled "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems" ("the AFR Guidance"). The guidance explains the roles of the Surveillance Camera Commissioner and Information Commissioner in relation to the regulation of the police use of AFR. The Surveillance Camera Commissioner AFR Guidance is designed to assist relevant authorities in complying with their statutory obligations "arising under section 31(1)" of the PFA 2012 and the SC Code (paragraph 1.3).

34. The AFR Guidance was promulgated on the basis that the Surveillance Camera Commissioner "should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems" (SC Code, paragraph 5.6). It is said that the AFR Guidance indicates "the way in which the Commissioner is minded to construe the particular statutory provisions arising from PFA 2012 and those provisions within the Code of Practice in the absence of case law" (paragraph 1.8).

35. The 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 Surveillance Camera Commissioner's 'Self-Assessment Tool'. In respect of watchlists there are suggestions concerning the nature of images used to produce watchlists.

36. Unlike the SC Code, there is no requirement for SWP to have regard to the AFR Guidance. This guidance was first published in October 2018 and re-published without changes in March 2019 (i.e. after the two deployments of AFR about which the Appellant complains).

SWP Documents

SWP Policy Document

37. SWP have issued a policy document entitled "Policy on Sensitive Processing of Law Enforcement Purposes, under Part 3 Data Protection Act 2018" (Version 2.0, November 2018) ("the November 2018 Policy Document"). That Policy Document sets out SWP's policy as regards compliance with the six Data Protection Principles in Part 3 of the DPA 2018:

> "**3. Compliance with Data Protection Principles**

a) 'lawfulness and fairness'

The lawfulness of South Wales Police processing is derived from its official functions as a UK police service, which includes the investigation and detection of crime and the apprehension of offenders, including acting in obedience to court warrants that require the arrest of defendants who have failed to attend court.

b) 'data minimisation'

South Wales police only processes sensitive personal data when permitted to do so by law. Such personal data is collected for explicit and legitimate purposes such as biometric data during the deployment of Automatic Facial Recognition technology.

c) 'accuracy'

During AFR Locate deployments South Wales Police collects the information necessary to determine whether the individual is on a watchlist. If an intervention is made the process will not prompt data subjects to answer questions and provide information that is not required.

Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified data sets.

d) 'storage limitation'

Providing complete and accurate information is required when constructing a watchlist. During AFR Locate deployments watchlists will be constructed on the day of deployment and where the deployments extend beyond 24 hours these will be amended daily. Where permitted by law and when it is reasonable and proportionate to do so, South Wales Police may check this information with other organisations – for example other police and law enforcement services. If a change is reported by a data subject to one service or a part of South Wales Police, whenever possible this is also used to update the AFR application, both to improve accuracy and avoid the data subject having to report the same information multiple times.

e) 'integrity and confidentiality'

South Wales Police has a comprehensive set of retention policies in place which are published online, further information specific to AFR can be found on SWP AFR webpage.

All staff handling South Wales Police information are security cleared and required to complete annual training on the importance of security, and how to handle information appropriately.

> In addition to having security guidance and policies embedded throughout SWP business, SWP also has specialist security, cyber and resilience staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access."

SWP Standard Operating Procedures ("SOP")

38. SWP has Automatic Facial Recognition SOP which apply to their use of AFR. They were published in November 2018 (i.e. after the dates of the 2 events in question), when a separate facial recognition section was added to SWP's website, and the SOPs were published on that webpage. The SOP's primary features include (see especially pages 6 and 14):

(1) A stipulation that watchlists should be "proportionate and necessary" for each deployment and primary factors for the inclusion on watchlists include will be "watchlist size, image quality, image provenance and rationale for inclusion".

(2) The numbers of images included within a watchlist cannot exceed 2,000 due to contract restrictions "but in any event1 in 1000 false positive alert rate should not be exceeded".

(3) Children under the age of 18 will not normally feature in a watchlist due to "the reduced accuracy of the system when considering immature faces".

(4) The decision for an AFR deployment wherever possible will ultimately be made by the Silver Commander.

(5) The rationale for the deployment of AFR is to be recorded in a pre-deployment report.

(6) Signs advertising the use of the technology are to be deployed to ensure that where possible an individual is aware of the deployment before their image is captured.

(7) Interventions are not to be made on the basis of a similarity score alone and when an intervention is made intervention officer will establish the identity of the individual by traditional policing methods.

(8) Details of the retention of different types of information gathered during an AFR deployment.

SWP Operational Advice

39. SWP have also issued guidance in the form of "Operational Advice for Police Trials of Live Facial Recognition" for use by officers conducting the trials which has been submitted to the National Police Chiefs Council.