Neutral Citation Number: [2019] EWHC 2341 (Admin)

Case No: CO/4085/2018

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
DIVISIONAL COURT
SITTING AT CARDIFF CIVIL JUSTICE CENTRE

2 Park Street, Cardiff, CF10 1ET

Date: 04/09/2019

Before:

LORD JUSTICE HADDON-CAVE
MR. JUSTICE SWIFT

- -

Between:

THE QUEEN (on application of EDWARD BRIDGES)	**Claimant**
- and -	
THE CHIEF CONSTABLE OF SOUTH WALES POLICE	**Defendant**
-and-	
SECRETARY OF STATE FOR THE HOME DEPARTMENT	**Interested Party**
-and-	
INFORMATION COMMISSIONER	
-and-	
SURVEILLANCE CAMERA COMMISSIONER	
	Interveners

- - - - - - - - - - -

Dan Squires QC and Aidan Wills (instructed by Liberty) for the **Claimant**
Jeremy Johnson QC (instructed by South Wales Police) for the **Defendant**
Richard O'Brien (instructed by Government Legal Department) for the **Interested Party**
Gerry Facenna QC and Eric Metcalfe (instructed by the Information Commissioner) for the **1st Intervener**
Andrew Sharland QC (written submissions only, instructed by Government Legal Department) for the **2nd Intervener**
Hearing dates: 21st May to 23rd May 2019

- -

JUDGMENT

Lord Justice Haddon-Cave and Mr. Justice Swift:

A. INTRODUCTION

1. The algorithms of the law must keep pace with new and emerging technologies. This case raises novel and important issues about the use of Automated Facial Recognition technology ("AFR") by police forces. The central issue is whether the current legal regime in the United Kingdom is adequate to ensure the appropriate and non-arbitrary use of AFR in a free and civilized society. At the heart of this case lies a dispute about the privacy and data protection implications of AFR. Counsel inform us that this is the first time that any court in the world had considered AFR.

Representation

2. The Claimant was represented by Dan Squires QC and Aidan Wills. The Defendant ("the SWP") was represented by Jeremy Johnson QC. The Interested Party, the Secretary of State for the Home Department was represented by Richard O'Brien. The Interveners were represented respectively, by Gerry Facenna QC and Eric Metcalfe (for the Information Commissioner), and Andrew Sharland QC (for the Surveillance Camera Commissioner). We are grateful to all counsel and their legal teams for the extensive research and work that has gone into preparing the detailed written and oral submissions and for the co-operative, helpful and able way in which this case has been presented on all sides. The parties have brought these proceedings before the Court in order to seek the Court's early guidance as regards the legal parameters and framework relating to AFR, whilst it is still in its trial phase, and before it is rolled-out nationally. We commend the spirit in which these proceedings have been brought and fought on all sides.

Introductory observations

3. At the beginning of his submissions for SWP, Mr Johnson QC pointed out that it was fifty years since the establishment of the SWP. Fifty years ago, the world of forensics and policing was very different. The ability of the police to identify people suspected of criminal offences was largely limited to fingerprint or eyewitness evidence. Advances in modern technology have led to dramatic advances in forensic policing, in particular: the forensic use of deoxyribonucleic acid ("DNA") evidence; closed circuit television ("CCTV") evidence which is ubiquitous; automatic number-plate recognition technology ("ANPR") which is widely used by police forces around the country; and cell-site evidence ("cell-site") which is a feature of many police investigations.

4. Each advance has naturally given rise to civil liberty concerns. It was never seriously suggested, however, that the police should not be able to make use of those technologies, so long as their use was in accordance with the law. Specific legislative measures were brought into effect in relation to the forensic use of fingerprints, DNA and CCTV (see *e.g.* the Police and Criminal Evidence Act 1984 and the Protection of Freedoms Act 2012). By those measures, and through scrutiny by the Courts of the ways in which such information is gathered, used and retained, the law seeks to strike a sensible balance between the protection of private rights, on the one hand, and the

public interest in harnessing new technologies to aid the detection and prevention of crime, on the other.

5. These competing objectives are readily apparent from the leading cases. Lord Steyn's introductory observations in his speech in *R(S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196, which concerned DNA, emphasised the public benefits in law enforcement agencies using new technology at [1]- [2]:

> "1. It is of paramount importance that the law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected and the innocent to be rapidly eliminated from inquiries. Thus, in the 1990s closed circuit television (CCTV) became a crime prevention strategy extensively adopted in British cities and towns. The images recorded facilitate the detection of crime and prosecution of offenders. Making due allowance for the possibility of threats to civil liberties, this phenomenon has had beneficial effects.
>
> 2. The use of fingerprint evidence in this country dates from as long ago as 1902. In due course other advances of forensic science followed. But the dramatic breakthrough was the use of DNA techniques since the 1980s. The benefits to the criminal justice system are enormous. For example, recent Home Office statistics show that while the annual detection rate of domestic burglary is only 14%, when DNA is successfully recovered from a crime scene this rises to 48%. It is, of course, true that such evidence is capable of being misused and that courts must be ever watchful to eliminate risks of human error creeping in. But as a matter of policy it is a high priority that police forces should expand the use of such evidence where possible and practicable."

6. The counterpoint is readily apparent from Lord Reed's observations in *R(T) v Chief Constable of Greater Manchester* [2015] AC 49 at [88]:

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

> The protection offered by the common law in this area has, by comparison, been of a limited nature."

7. AFR is another new and powerful technology which has great potential to be put to use for the prevention and detection of crime, the apprehension of suspects or offenders and the protection of the public. Its use by public authorities also gives rise to significant civil liberties concerns. Using AFR can involve processing the facial biometric data of large numbers of people. The raw power of AFR - and the potential baleful uses to which AFR could be put by agents of the state and others - underline the need for careful and on-going consideration of the effectiveness of that framework as and when the uses of AFR develop. The judgment in this case is directed specifically to the way in which the technology has been used to date by SWP, in the form of a pilot project known as "AFR Locate". Put very shortly, 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 watchlists compiled by SWP for the purpose of the deployment. The debate in these proceedings has been about the adequacy of the current legal framework in relation to AFR Locate.

The Parties

8. The Claimant is Edward Bridges, a civil liberties campaigner who lives in Cardiff. He brings this claim supported by Liberty, the well-known independent civil liberties membership organisation. The Defendant is the Chief Constable of South Wales Police (*Heddlu De Cymru*). SWP is the national lead on the use of AFR in policing in the UK and has been responsible for conducting trials of the technology since mid-2017.

9. 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 has published a Biometrics Strategy[1] and created an Oversight and Advisory Board to co-ordinate consideration of the use of facial images and AFR technology by law enforcement authorities. The Information Commissioner has specific statutory powers and responsibilities under the Data Protection Act 2018 ("DPA 2018")[2], and had like 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 s.34 of the Protection of Freedoms Act 2012 ("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.

---

1 Home Office Biometrics Strategy (June 2018)

2 Part 5 and Schedules 12 and 13 of the Data Protection Act 2018

B. THE CLAIMS

10. The Claimant challenges the lawfulness of SWP's use of AFR Locate generally and complains regarding two particular occasions when AFR Locate was used in Cardiff by SWP when he was present. Both occasions were part of the trial being undertaken by SWP. The trial period has not yet been completed. The first use of AFR Locate by SWP took place in June 2017 when the UEFA Champions League Final took place at the Principality Stadium. The particular deployments in issue in these proceedings were (a) on 21st December 2017 at Queen Street, a busy shopping area in Cardiff; and (b) on 27th March 2018 at the Defence Procurement, Research, Technology and Exportability Exhibition ("the Defence Exhibition") which was held at the Motorpoint Arena. The Claimant claims to have been present and to have been caught on camera on each of these two occasions.

21st December 2017 deployment

11. On 21st 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. Inspector Lloyd explained that AFR was deployed that day primarily to locate and detain wanted "Priority and Prolific Offenders". There were three watchlists for this deployment: (a) a "red" watchlist, comprising one person suspected of having committed a serious crime, (b) an "amber" watchlist, comprising 382 people wanted on warrant, and (c) a "purple" watchlist, comprising 536 suspects (in effect, every person suspected of committing a crime in the SWP area). The watchlists therefore totalled 919 people. There were 10 possible matches during the deployment. Of these 2 were not true matches. In one of those cases there was no intervention. Of the 8 true matches there were 2 arrests.

12. The Claimant says he was present at Queen's Street on 21st December 2017. He says that he was approximately 6-10 feet from the van and was, accordingly, in range of the cameras. The Claimant 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.

27th March 2018 deployment

13. On 27th March 2018, the Defence Exhibition took place at the Motorpoint Arena in Cardiff. Inspector Lloyd explained that AFR was deployed because 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 focussing on the arena's entrance.

14. There were again three watchlists: (a) a "red" watchlist, comprising 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; (b) an "amber" warrant watchlist, comprising 347 persons wanted on warrants; and (c) a "purple" watchlist, comprising 161 suspects (linked to crimes in the SWP 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 6 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.

15. The Claimant's evidence is 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, albeit at one point he walked along the pavement in front of the arena and would have been closer than that. Prior to seeing the van, he was not aware that AFR was in use. He did not observe SWP officers providing any information about the use of AFR.

16. It is not now possible for SWP to check either whether the Claimant's image was recorded by CCTV on 21st December 2018 or 27th March 2018, or whether his facial biometric information was processed by the AFR system on either occasion. If this data was processed, then the technology would have identified that the Claimant was not a person of interest who was included on the watchlist for either of these deployments. His biometric data and facial image would have been immediately deleted from the AFR system. He has not been included on an SWP watchlist in its deployments of AFR to date. SWP does not hold any of his personal data (except as a result of these proceedings).

Claimant's standing, and grounds of challenge

17. Notwithstanding this, SWP does not seek to challenge the Claimant's standing to bring these judicial review proceedings; and SWP does not dispute that the Claimant is a victim for the purposes of section 7 of the Human Rights Act 1998. For pragmatic reasons, SWP accepts the Claimant's evidence that he was present at Queen's Street and at the Motorpoint Arena, and that on those occasions his image was recorded.

18. The Claimant's overall contention is that SWP's use of AFR Locate, on the two occasions referred to above and generally, is contrary both to Convention rights (Ground 1) and the requirements of data protection legislation (Ground 3). The Claimant also contends that when deciding to implement use of AFR Locate, SWP failed to comply with the public-sector equality duty (*i.e.* the obligation on public authorities such as SWP, under section 149(1) of the Equality Act 2010, to have "due regard" to certain prescribed matters when exercising their functions) (Ground 4). We refer to these below as (1) the Convention Rights Claim, (2) the Data Protection Claims, and (3) the Public-Sector Equality Duty Claim, respectively.

19. As to the Convention Rights Claim, the Claimant contends that using AFR Locate is an interference with his rights under ECHR article 8(1); and that, for

the purposes of Article 8(2) the interference is neither "in accordance with the law" nor "necessary" or "proportionate". [3]

20. The Data Protection Claims are brought both under the DPA 1998 and under the DPA 2018. The latter superseded the former with effect from 25 May 2018. The claim under the DPA 1998 is that by using AFR Locate on Queen Street on 21st December 2017, and at the Motorpoint Arena on 27th March 2018, SWP acted contrary to section 4(4) of that Act by failing to act in accordance with the data protection principles. The claim under the DPA 2018 is in two parts:

    (1) The first part is that any current or future use by SWP of AFR Locate would fail to comply with section 35 of that Act. Section 35 is within Chapter 2 of Part 3 of the DPA 2018, which applies to law enforcement processing by "competent authorities". SWP is such an authority. A failure to comply with section 35 (which sets out the first data protection principle) would be a breach of the obligation at section 34(3) of the Act which requires SWP to be able to demonstrate compliance with the requirements of Chapter 2 of Part 3 of the DPA 2018.

    (2) The second part is that the use of AFR Locate is processing that falls within section 64(1) of the DPA 2018, and that SWP has failed to comply with the requirement under that section to carry out a data protection impact assessment.

21. The Public Sector Equality Duty Claim (under section 149(1) of the Equality Act 2010) is that it is evident from the equality impact assessment document created by SWP in April 2017, in respect of its then proposed use of AFR Locate, that it failed to have regard to the possibility that use of the AFR software would produce a disproportionately higher rate of false positive matches for those who are women or from minority ethnic groups, such that use of AFR Locate would indirectly discriminate against those groups. That failure, says the Claimant, means that SWP failed to have the required due regard for any of the relevant considerations prescribed at section 149(1)(a) – (c) of the 2010 Act.

22. For ease of reference, we set out in **ANNEX "A"** to this judgment the relevant legal framework under consideration comprising:

(1) Legislation

- Data Protection Act 1998 ("DPA 1998")
- Protection of Freedoms Act 2012 ("PFA 2012")
- The Law Enforcement Directive
- Data Protection Act 2018 ("DPA 2018")

---

[3] Ground 2 (breach of Articles 10 and 11 ECHR) was withdrawn.

(2) Code and Guidance

- Secretary of State's Surveillance Camera Code of Practice
- Surveillance Camera Commissioner's AFR Guidance

(3) SWP Documents

- SWP Policy Document
- SWP Standard Operating Procedures ("SOP")
- SWP Operational Advice

C. AFR TECHNOLOGY

23. In simple terms, AFR[4] 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. The present case is concerned with what is described by SWP as "AFR Locate", which we describe below.

24. In slightly more detail, the technical operation of AFR comprises the following 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 therein. In order for such images to be used for AFR, they are processed so that the "facial features" associated with their subjects are extracted and expressed as numerical values.

(2) Facial image acquisition. A CCTV camera (which could be mounted on *e.g.*, a van, lamp post or contained in a handheld device) takes digital pictures of facial images in real time. This may be done by (i) taking a static photograph in a "controlled" environment (for example where an individual has her photograph taken at a border gate when presenting a passport); or (ii) capturing a moving image when a person passes into the camera's field of view, using a live feed. This case is concerned with the latter, *i.e.* the use of AFR cameras in real time, in a "live" context.

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

---

[4] Also known as Facial Recognition Technology, Automatic Facial Recognition Technology, and (when used in real time, in a live setting) Live Facial Recognition.

(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. It is common to suggest setting the threshold value so that the False Alarm Rate is 0.1%, 0.01% or 0.001%. Most AFR systems, however, allow the end user to change the threshold value to whatever they choose. However, operators of AFR systems are able to amend the "threshold [of similarity] value", above which a similarity score is taken to indicate a potential match.

25. Thus, whilst use of CCTV cameras is a premise for use of AFR, AFR technology goes further. A CCTV camera simply captures digital video recordings. AFR technology uses that digital information to isolate pictures of individual faces, extract information about facial features from those pictures, compare that information with the watchlist information, and indicate matches between faces captured through the CCTV recording and those held on the watchlist.

D. SWP's USE OF AFR

26. SWP is the police authority which is the national lead on testing and conducting trials of AFR. The SWP has received grants from the Secretary of State for this purpose. The SWP has used AFR since mid-2017, and continues to use it. SWP has a licence to use proprietary AFR software developed by NEC (now North Gate Public Services (UK) Ltd) called "NeoFace Watch software".

27. SWP uses AFR in two ways[5]. The first is known as "AFR Identify" under which images of unknown suspects and persons of interest related to past

[5] See, the Evaluation of South Wales Police's Use of Automatic Facial Recognition (Cardiff University, Police Science Institute, Crime & Security Research Institute) (September 2018) ("the UPSI Report") at pp. 2, 12-15.

crimes or incidents, are compared against images in the SWP custody database (which contains approximately 500,000 pictures). This use of AFR is not in issue in these proceedings.

28. The second use of AFR is referred to by SWP as "AFR Locate", which as we have said, is the subject of the claim in this case. SWP has deployed AFR Locate on about 50 occasions between May 2017 and April 2019 at a variety of large public events, including on the day of the 2017 UEFA Champions League Final, at various international rugby matches at the Principality Stadium, at pop concerts and at an Elvis Presley Festival. The deployment on 31st May 2017, on the day of the UEFA Champions League Final led to the first arrest from a real-time AFR deployment (of a wanted domestic violence offender).

29. When AFR Locate is deployed, digital images of faces of members of the public are taken from live 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.

30. 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 (a) persons wanted on warrants, (b) individuals who are unlawfully at large (having escaped from lawful custody), (c) persons suspected of having committed crimes, (d) persons who may be in need of protection (*e.g.* missing persons), (e) individuals whose presence at a particular event causes particular concern, (f) persons simply of possible interest to SWP for intelligence purposes and (g) vulnerable persons[6].

31. In relation to persons placed on a watchlist on suspicion of having committed an offence and persons wanted on a warrant, there is (subject to the overarching requirements of proportionality and necessity) no minimum threshold of seriousness for the types of offences the person committed or is suspected of committing. The inclusion of persons on a watchlist on suspicion of having committed an offence and/or person wanted on a warrant is not dependent upon the existence of any specific basis for suspecting that that individual is likely to be present at the location at which AFR is deployed, save that SWP's current practice is that they will be suspected of offending in the South Wales area (or wanted on a warrant issued by a South Wales court). Bespoke watchlists may, however, be created for intelligence purposes where it is considered likely that a person will be at the location of a particular deployment. To date, the watchlists used by SWP have comprised between 400-800 people. The maximum capacity for a watchlist is 2,000 images.

---

6 See also, the UPSI Report, at p. G/177 of the hearing bundle. SWP says that in practice "intelligence" in this context means knowledge of the attendance of the particular individual at the particular event for the purpose of the prevention and detection of crime.

32. The watchlist images are "enrolled" into the AFR system, meaning that a biometric template is taken from the images which will then be used for the purposes of undertaking algorithmic comparisons with the facial biometrics of members of the public captured on camera.

33. 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 believes that a match has in fact been made. In our view, the fact that human eye is used to ensure that an intervention is justified, is an important safeguard. 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, he believes there is a match, he may inform other officers stationed nearby who will intervene ("intervention officers"). SWP says that those officers will themselves make their own assessment and will only intervene if satisfied that the person may be the subject of interest. SWP have developed a 'traffic light' system with colours (red, amber and green) to delineate the urgency and type of intervention required. 'Red' indicates the need for an immediate response because, *e.g.,* of a counter-terrorist threat, 'amber' indicates the need for an arrest intervention, and 'green' indicates the need for an identification for intelligence development purposes only. If the person identified is on a 'red' watchlist, the system operator may be given instructions to contact the person responsible for the decision that that person should be placed on the watchlist and to obtain instructions as to what action should be taken.

34. Deployment locations are generally selected as being places at which SWP can maximise the number of faces scanned in a given deployment. In addition, deployment locations may be selected on the basis that they are locations or events associated with attracting disorder or criminal activity. When AFR is deployed, the SWP mounts CCTV cameras on stationary, or mobile police vehicles, or on poles or posts, so to capture images of the face of anyone who passes within range of the camera.

35. SWP has consulted with the Surveillance Camera Commissioner on the use of CCTV cameras. The CCTV camera records footage for the duration of any AFR Locate deployment. AFR Locate is capable of scanning 50 faces per second (albeit that does not necessarily mean 50 different people). Beyond these 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 enrol and therefore process as many individuals as possible[7].

36. Whilst SWP does not routinely record the total number of people whose facial biometrics are captured and processed as part of each deployment of AFR, it is clear that these numbers are very large (*e.g.* approximately 21,500 faces were scanned at a Rugby Union international in November 2017, and approximately 44,500 during the course of a weekend event in Swansea). Over the 50

---

[7] SWP Data Protection Impact Assessment (p.19)

deployments that were undertaken in 2017 and 2018, around 500,000 faces may have been scanned (albeit not necessarily 500,000 different individuals). AFR Locate is currently set to detect up to five faces in a given frame and may capture 10 frames per second. The overwhelming majority of persons whose biometrics are captured and processed by SWP using AFR Locate are not suspected of any wrongdoing.

Data retention

37. 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.

38. SWP's Standard Operating Procedures[8] and Data Protection Impact Assessment provide for data retention periods. These are kept under review. The current data retention periods are in summary:

    (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 when AFR Locate is used

39. 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 which they may be attending or present. These steps are set out in the statement of Inspector Lloyd of the Digital Services Department of SWP. They include as follows:

---

[8] Published in November 2018

(i) 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; (ii) 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 (iii) handing out of 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.[9] Inspector Lloyd further explains

> "30. … It is important to ensure that a balance is maintained between transparency and engagement whilst not unduly impacting on the effectiveness of the deployment. This balance is achieved via a risk-based approach, at times it may be appropriate to advertise a deployment so that individuals of concern are deterred from attending. At other times it may be more appropriate to encourage attendance by not disclosing deployment specifics so that an individual is more likely to attend and be detained."

40. Whilst deployment of AFR is not covert, it is reasonable to suppose, however, 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

41. The use of AFR technology involves the collection, processing and storage of a wide range of information, including (i) facial images, (ii) facial features (*i.e.* biometric data), (iii) metadata, including time and location, associated with the same and (iv) 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 Secretary of State's Biometrics Strategy (June 2018) as "the recognition of people based on measurement and analysis of their biological characteristics or behavioural data" [10].

42. 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. The Biometrics Strategy (June 2018) explains that "biometrics have long provided a critical role across the Home Office sector from traditional policing forensics, immigration services to national security"[11].

43. Facial biometrics bear some similarity to fingerprints because (a) both can be captured without the need for any form of intimate sampling and (b) both concern a part of the body that is generally visible to the public (*c.f.* C-291/12

---

9 http://afr.south-wales.police.uk/

10 Home Office *Biometrics Strategy - Better Public Services Maintaining Public Trust* (*June 2018*) (para.1)

11 *Ibid* (para.2)

Schwarz v Stadt Bochum [2014] 2 CMLR 5 at [48]). However, by the use of AFR technology, facial biometrics can be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale.

44. The Secretary of State has set up an Oversight and Advisory Board, comprising representatives from the police, 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.

E. THE CONVENTION RIGHTS CLAIM

45. The Claimant contends that SWP's use of AFR Locate is in breach of the requirements of ECHR Article 8. Article 8 provides as follows:

> "Article 8
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

46. AFR permits a relatively mundane operation of human observation to be carried out much more quickly, efficiently and extensively. It is technology of the sort that must give pause for thought because of its potential to impact upon privacy rights. As the Grand Chamber of the Strasbourg Court said in *S v. United Kingdom* (2009) 48 EHRR 50 at [112]:

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

(1) Has there been an interference with the Claimant's Article 8(1) rights?

Reach of Article 8(1)

47. It is now well-established that the reach of Article 8(1) is broad. The notion of "private life" is not susceptible to exhaustive definition. It covers the "physical and psychological integrity" of a person. A person's private and family life can therefore embrace multiple aspects of a person's "physical and social identity", including (relevantly in the present case), *e.g.* gender, name, other means of personal identification and of linking to a family, ethnic identity, and elements relating to a person's right to their image (*S v. United Kingdom* (2009) 48 EHRR 50, at [66]; *Von Hannover v. Germany* (2004) 40 EHRR 1, at [50] (cited by Lord Toulson in *Re JR 38* [2016] AC 1131 at [84])).

48. The phrases "physical and psychological integrity" and "physical and social identity" are the central value protected by Article 8 and have been described as the "personal autonomy of every individual… [which] marches with the presumption of liberty enjoyed in a free polity; a presumption which consists in the principle that every interference with the freedom of the individual stands in need of objective justification" (*per* Laws LJ in *R(Wood) v. Commissioner of Police of the Metropolis* [2010] 1 WLR 123 at [20]-[21], (cited by Lord Toulson in *Re JR 38 , ibid,* at [86])).

49. Yet the reach of Article 8(1) is not without limit. In *R(Wood) v. Commissioner of Police of the Metropolis, ibid,* at [22], (cited with approval by Lord Toulson in *Re JR 38, ibid,* at [86])), Laws LJ stated as follows

> "22. This cluster of values, summarised as the personal autonomy of every individual and taking concrete form as a presumption against interference with the individual's liberty, is a defining characteristic of a free society. We therefore need to preserve it even in little cases. At the same time, it is important that this core right protected by article 8, however protean, should not be read so widely that its claims become unreal and unreasonable. For this purpose, I think there are three safeguards, or qualifications. First, the alleged threat or assault to the individual's personal autonomy must (if article 8 is to be engaged) attain "a certain level of seriousness". Secondly, the touchstone for article 8(1)'s engagement is whether the claimant enjoys on the facts a "reasonable expectation of privacy" (in any of the senses of privacy accepted in the cases). Absent such an expectation, there is no relevant interference with personal autonomy. Thirdly, the breadth of article 8(1) may in many instances be greatly curtailed by the scope of the justifications available to the state pursuant to article 8(2). …"

Submissions

50. On behalf of the Claimant, Mr Squires submitted that use of AFR entailed interference with the Claimant's Article 8 rights. The Claimant was in a public place engaged in lawful activities, and was not suspected of any wrongdoing. Obtaining and using his facial biometric information (a unique identifier), without his consent, is at odds with the protection afforded by Article 8(1).

51. On behalf of SWP, Mr Johnson submitted that the Claimant could not establish any interference with his rights under Article 8(1) for essentially four reasons. The first reason was that there was no proof that the Claimant's image had been captured by the AFR on either occasion. If that were the case that would be a complete response to the Claimant's case. Ultimately, however, and for pragmatic reasons (so that the Court would address the substantive legal issues raised), Mr Johnson was willing to accept that it was more likely than not that on one or other occasion the Claimant's image had been captured and processed. The second, third and fourth reasons were closely linked: that a person could not have a reasonable expectation of privacy when walking in a public place and could expect his image to be recorded for crime prevention purposes; that AFR was a near-instantaneous process and a person's biometric data is not recorded and is never available to a human operator; and that overall, taking a picture in such circumstances and processing the digital information obtained from it in that manner did not meet the minimum threshold of seriousness required by Article 8(1).

Discussion

52. We do not accept the SWP's submissions on this issue. As to the first point, even if the pragmatic concession we have referred to had not been made, we would have concluded that the Claimant has proved that he was within reasonable proximity of the CCTV cameras on the days and at location in question when AFR technology was deployed by SWP, namely on 21st December 2017 at Queen Street and on 27th March 2018 at the Arms Fair. Notwithstanding that the CCTV footage for each occasion was deleted well before these proceedings were commenced (such footage is routinely deleted after 31 days), the Claimant's physical proximity to the location of the cameras on both days is sufficient to give rise to a reasonable apprehension that his image may have been captured and processed on one or both occasions such as to entitle him to claim a violation of his Article 8 rights, either as an individual present himself or as a member of a class of people who risked being directly affected by the SWP's use of AFR on either of those occasions (c.f. Lord Reed, in *AXA General Insurance v. HM Advocate* [2011] UKSC 46; [2012] 1 AC 868 at [111]).

53. In *Wood*, Laws LJ rejected the submission that the "bare act of taking pictures" amounted to an interference with Article 8(1) rights (see [36] and [37]). He pointed to the need for what he described as "aggravating circumstances". In that case, and in the context of police activity, he suggested that where state actions complained of were "expected and unsurprising", it

might well be that such actions might entail no breach of Article 8(1). At paragraph 43 he stated as follows.

> "In *R(Gillan) v Commissioner of Police for the Metropolis* ... [2006] 2 AC 307 at [28] …] Lord Bingham referred to "an ordinary superficial search of the person and an opening of bags, of the kind to which passengers uncomplainingly submit at airports": another instance in which the putative violation of Article 8 (if any violation were suggested) consists in something familiar and expected. In cases of that kind, where the police or other public authority are acting just as the public would expect them to act, it would ordinarily no doubt be artificial and unreal for the courts to find a *prima facie* breach of Article 8 and call on the State to justify the action taken by reference to Article 8(2)."

In substance, SWP's remaining points were to the effect that, qualitatively, its use of AFR Locate was an activity of similar nature.

54. We cannot see how what happened can be characterised in this way. AFR Locate goes much further than the simple taking of a photograph. The digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information. The fact that this happens when the Claimant is in a public space is not a sufficient response. In *PG v United Kingdom* (2008) 46 EHRR 51, the European Court of Human Rights stated as follows (at [57]):

> "57. There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectation as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain …" (emphasis added)

55. The extraction and use of the Claimant's biometric data takes the present case well beyond the "expected and unsurprising". In *S v. United Kingdom* (*supra),* the European Court of Human Rights emphasised the significance of the protection of personal data as part of protecting Article 8 rights. The Court said (at [67] and [103]) (emphasis added):

> " 67. The mere storing of data relating to private life of an individual amounts to an interference within the meaning of art.8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above [*e.g.* aspects of the persons physical and social identity], the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained."
>
> "103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by art.8 of the Convention. …"

(*c.f* also *Satakunnan Markkinaporssi Oy v Finland* (2018) 66 EHRR 8 at [137]).

56. In *S v. United Kingdom,* the Court was concerned with the retention of biometric information in the form of fingerprint records and DNA samples. It recognised that each comprised a source of unique information about a person. We note in particular what the Court said in respect of fingerprints since they are clearly a source of significantly less personal data than a DNA sample. In the context of rejecting an argument that retention of fingerprints did not involve any interference with Article 8(1) rights because fingerprint analysis was an expert process, the Court said (at [84]):

> "84. … While true, this consideration cannot alter the fact that fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant."

57. For the purposes of the Article 8(1) argument, the same reasoning applies to AFR technology. 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. Taken alone or together with other recorded metadata, AFR-derived biometric data is an important source of personal information. Like fingerprints and DNA, in the language later used by the Court at paragraph 104, it is information of an "intrinsically private" character. The fact that the biometric

data is derived from a person's facial features that are "manifest in public" does not detract from this. The unique whorls and ridges on a person's fingertips are observable to the naked eye. But this does not render a fingerprint any the less a unique and precise identifier of an individual. The facial biometric identifiers too, are precise and unique.

58. The Court of Justice of the European Union ("CJEU") has also repeatedly emphasised that the right to protection of personal data is "closely connected with the right to respect for private life", and that "the right to respect for private life with regard to the processing of personal data" is founded on both Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and extends to "any information relating to an identified or identifiable individual" (C-468/10 and C-469/10 *ASNEF v Administración del Estado* [2012] 1 CMLR 48 at [41] – [42]; see also C-291/12 *Schwarz v Stadt Bochum* [2014] 2 CMLR 5 at [26] which concerned a person's refusal to provide his fingerprints in the context of obtaining a passport). The CJEU noted that fingerprints "objectively contain unique information about individuals which allows those individuals to be identified with precision" (at [27]). It held that both the taking and retention of fingerprints "constitutes a threat to the rights to respect for private life" (at [30]). The Court went on to hold that the taking of fingerprints and facial images engaged Articles 7 and 8 of the Charter (at [49]).

59. The fact that, save where a match is detected, facial biometric information is retained for only a very short period, does not affect the analysis. The application of Article 8 is not dependent on the long-term retention of biometric data. It is sufficient if biometric data is captured, stored and processed, even momentarily. The mere storing of biometric data is enough to trigger Article 8 and the subsequent use (or discarding) of the stored information has no bearing (see *S v. United Kingdom* at [67], above). Accordingly, the fact that the process involves the near instantaneous processing and discarding of a person's biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter. The AFR process still necessarily involves the capture, storage and "sensitive processing" of an individual's biometric data before discarding. Article 8 is triggered by the initial gathering of the information. In the context of the interception of communications, the Strasbourg Court has treated the initial gathering of the information in question, its retention, and any subsequent use, as discrete interferences with Article 8 (see *Amann v Switzerland* (2000) 30 EHRR 843 [GC] at [48] and [69]).

60. We are fortified in our conclusion that the use of AFR technology engages Article 8 by the fact that our view is shared by both the Information Commissioner and the Surveillance Camera Commissioner. The Information Commissioner stated in her skeleton argument:

> "18. … The automated capture of facial biometrics, and conversion of those images into biometric data, involves large scale and relatively indiscriminate processing of personal data. If such processing is not

> subject to appropriate safeguards, such data … could be collected … in a manner amounting to a serious interference with privacy rights."

61. The Surveillance Camera Commissioner's AFR Guidance states that Article 8 is a "fundamental consideration" in the context of the "overt operation of surveillance camera systems"; and the "use of AFR … in crowded places and selected sites will significantly enhance the capabilities of a surveillance camera system to intrude and gather private information of a citizen" (paragraphs 2.1 – 2.2). He refers to the "intrusive capabilities of AFR" (paragraph 9.2) and expresses the view that "potential for intrusion arising from AFR is arguably consistent with that arising from some forms of covert surveillance tactics and capabilities" (paragraph 10.2). It is clear that this is not confined to persons whose images are contained on watchlists.

62. For these reasons, in our view, the use of AFR Locate does entail infringement of the Article 8(1) rights of those in the position of the Claimant in this case. The points we have made above have focussed on the position of members of the public, such as the Claimant whose images are digitally recorded by CCTV, and then processed by the AFR Locate technology. For sake of completeness we note that the effect, in Article 8(1) terms, for those people who are on the watchlist, is the same, albeit that the information that is processed is drawn from a database of custody photographs held on SWP's Niche Record Management System. Neither SWP nor any other party before us sought to contend otherwise.

(2) Is the SWP's use of AFR in accordance with the law?

63. The Claimant's primary argument on his Article 8 case was that the use of AFR Locate by the SWP is not "in accordance with the law" for the purposes of Article 8(2). Mr Squires QC's submission was both to the effect: (a) that there is no legal basis for the use of AFR Locate, such that SWP does not, as a matter of law, have power to deploy it (or for that matter, to make any other use of AFR technology); and (b) that even if SWP's use of AFR Locate is not ultra vires, any interference with Article 8(1) rights is not subject to a sufficient legal framework such that it is capable of being justified under Article 8(2). In support of this latter argument, the Claimant contends that the generic legal framework provided, successively, by the DPA 1998 and the DPA 2018 is insufficient.

64. The Claimant points to the provisions of the Police and Criminal Evidence Act 1984 ("PACE"), and in particular to Code D "Revised Code of Practice for the Identification of Persons by Police Officers" issued under section 66 of PACE, and Annex F to Code D which he contends, collectively, regulate obtaining and use of fingerprints and DNA samples. His case is that absent comparable provision for AFR technology, its use is not in accordance with the law. If this requirement under Article 8(2) is to be satisfied, there must be a legal framework that specifies: (a) when AFR Locate may be deployed, for example only when there is "reasonable suspicion" or a "real possibility" that persons who are sought may be in the location where AFR Locate is deployed; (b)

where it may be deployed – the Claimant suggested only at places such as airports, or at large public gatherings such as sporting events; (c) the classes of persons who may be on a watchlist – the Claimant contends that watchlists should only include "serious criminals at large"; (d) the sources from where images included in watchlists may be obtained; and (e) clear rules relating to biometric data obtained through use of AFR Locate – for example as to how long it may be retained, and the purposes for which such information may (or may not) be used. In the context of the requirement under section 35(2) of the DPA 2018 that any processing of personal data must be "based on law", the Information Commissioner made a similar submission. Although she did not seek to limit the categories of persons who might be included on watchlists, her submission was that the categories of who could be included on a watchlist needed to be specified by law. She also submitted that the purposes for which AFR Locate could be used should be specified in law. Her overall submission was that both any use of AFR Locate, and any decision as to who should be included on a watchlist, needed to be the subject of "independent authorisation".

65. Mr Squires QC relied upon Lord Kerr's observation in his dissenting judgment in *Beghal v Director of Public Prosecutions* [2016] AC 88 at [102] that:

> " 102. … The fact that a power is exercised sparingly has no direct bearing on its legality. A power on which there are insufficient legal constraints does not become legal simply because those who may not 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."

66. He also drew attention to expressions of concern as to the adequacy of the legal framework governing the use of AFR technology by the police. In his Annual Report for 2017, the Biometrics Commissioner stated:

> "303. Given that [the Protection of Freedoms Act] is not generic legislation covering all biometrics used by the police, the use by the police of these second generation biometrics [which the Commissioner defined as including facial image matching] <u>is not currently governed by any specific legislation, other than general data protection legislation, and only by regulations drawn up by the police themselves</u> such as the Management of Police Information principles (MOPI) drawn up by the College of Policing. It is therefore the case that <u>technical development and deployment is running ahead of legislation, which is why the Home Office's promised biometric strategy is urgently needed</u>" (emphasis added)

67. In addition, the Claimant points to the following: (a) that the Secretary of State's Biometrics Strategy (June 2018) acknowledged that "governance and oversight of these [AFR] applications and the use of facial images as a biometric by law enforcement could be strengthened further"[12]; (b) that the Information Commissioner has expressed her concern "about the absence of national level co-ordination in assessing the privacy risks and a comprehensive governance framework to oversee [AFR] deployment."[13]; and (c) that the Surveillance Camera Commissioner queried the legal basis for the use of AFR and stated that he does not consider the existing legislation governing the use of AFR by police to be wholly satisfactory.[14]

(1) Legal basis for SWP's use of AFR: Is AFR Locate ultra vires the SWP?

68. The Claimant's first contention is that there must be some specific statutory basis for the use of AFR Locate – *i.e.* to permit the use of the CCTV cameras, and the use of the software that processes the digital information that the cameras collect. SWP and the Secretary of State rely on the police's common law powers as sufficient authority for use of this equipment.

69. The relevant principles at common law are well-established. First, a police constable is a creature of the common law[15]. Police constables owe the public a common law duty to prevent and detect crime. That duty reflects a corresponding common law power to take steps in order to prevent and detect crime. As Lord Parker CJ said in *Rice v Connolly* [1966] 2 QB 414 at 419B - C:

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

70. *Second*, this general power of the police includes the use, retention and disclosure of imagery of individuals for the purposes of preventing and detecting crime. In *R (Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123, the police took and retained photographs of the claimant in the street for the purpose of gathering evidence about possible disorder and criminal conduct. Laws LJ and Lord Collins held that this was lawful (see [50]-[55] and [98]-[100] respectively). As Lord Collins observed *ibid* at [98], "The taking of the photographs in the present case was lawful at common law, and there is nothing to prevent their retention".

---

12 Biometrics Strategy (June 2018), p.12.

13 Information Commissioner's Office, *Blog: facial recognition technology and law enforcement*.

14 See the *National Surveillance Camera Strategy for England and Wales*, para. 303.

15 See Halsbury's Laws, Vol 84 (Police and Investigatory Powers), paragraph 1.

71. In *R (Catt) v Association of Chief Police Officers* [2015] AC 1065, the Supreme Court considered the lawfulness of collecting and retaining personal information, including a photograph of an individual who had demonstrated against the operation of an arms manufacturer on a "domestic extremism" database. In relation to the police's power to obtain and hold such information, Lord Sumption JSC held at [7]:

> "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. These powers do not authorise intrusive methods of obtaining information, such as entry onto private property or acts (other than arrest under common law powers) which would constitute an assault. But they were amply sufficient to authorise the obtaining and storage of the kind of public information in question on these appeals." (emphasis added)

72. *Third*, the police may make reasonable use of a photograph of an individual for the purpose of the prevention and detection of crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large and may do so whether or not the photograph is of any person they seek to arrest or of a suspected accomplice or of anyone else. "The key is that they must have these and only these purposes in mind and must … make no more than reasonable use of the picture in seeking to accomplish them" (per Laws J in *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 at 810F).

73. It will be apparent from the passages highlighted in the judgments in *Rice* and *Catt*, that the extent of the police's common law powers has generally been expressed in very broad terms. The police did not need statutory powers, *e.g.* to use CCTV or use body-worn video or traffic or ANPR[16] cameras, precisely because these powers were always available to them at common law. Specific statutory powers were needed for *e.g.* the taking of fingerprints, and DNA swabs to obviate what would otherwise be an assault.

74. As we see matters, the only issue is whether using cameras fitted with AFR technology to obtain the biometric data of members of the public in public can be said to be an "intrusive method" of obtaining information in the sense referred to by Lord Sumption JSC in *Catt* (at [7] above) and, therefore, out-with the common law powers of the police. In our view, Lord Sumption was clearly referring to intrusion in the sense of *physical* intrusion or interference with a person's rights vis-à-vis their home or interference with their bodily integrity. He described "intrusive methods" as including "entry on private property or acts… which would constitute an assault".

75. A warrant is required to allow the police to enter someone's private property since otherwise, the act of entering someone's private property without permission would amount to a trespass,. Equally, since the act of taking

---

16 Automatic Number Plate Recognition cameras

fingerprints generally requires the cooperation of, or use of force on, the subject and would otherwise amount to an assault, statutory powers were enacted to enable the police to take fingerprints. Both involve physically intrusive acts. By contrast, the use of AFR Locate to obtain biometric information is very different. No physical entry, contact or force is necessary when using AFR Locate to obtain biometric data. It simply involves taking a photograph of someone's face and the use of algorithms to attempt to match it with photographic images of faces on a watchlist. The method is no more intrusive than the use of CCTV in the streets.

76. So far as watchlists are concerned, the lists in issue before us have comprised imagery acquired by way of police photography of arrested persons. The police have explicit statutory powers to acquire, retain and use such imagery (see s.64A Police and Criminal Evidence Act 1984).

77. As has been explained, the watchlists comprised "persons of interest" to the police. The Claimant was not on any SWP watchlist: for the purposes of section 7 of the Human Rights Act 1998, he is not a "victim" in this regard, and therefore can have no personal complaint about the watchlists. Nor can we see that there is any reasonable basis for complaint arising from the fact that watchlists used by SWP have included not just known criminals but persons of "possible interest" to SWP for intelligence purposes. The compilation of watchlists is something well within the common law powers of the police as enunciated *e.g.* by Lord Parker CJ in *Rice*, namely "all steps … necessary for keeping the peace, for preventing crime or for protecting property".

78. For these reasons, we consider the police's common law powers to be "amply sufficient" in relation to the use of AFR Locate. The police do not need new express statutory powers for this purpose.

(2) Is there a sufficient legal framework for the use of AFR Locate?

79. The Claimant's second submission is that there is no sufficient legal framework for the use of AFR Locate such that its use lacks the necessary qualities of foreseeability, predictability, and hence of legality. This requirement was explained by Lord Bingham in *R(Gillan) v Commissioner of Police of the Metropolis* [2006] 2 AC 307 at [34], as follows:

> " The lawfulness requirement in the Convention addresses supremely important features of the rule of law. The exercise of power by public officials, as it affects members of the public, must be governed by clear and publicly accessible rules of law. The public must not be vulnerable to interference by public officials acting on any personal whim, caprice, malice, predilection or purpose other than that for which the power was conferred. This is what, in this context, is meant by arbitrariness, which is the antithesis of

> legality. This is the test which any interference with or derogation from a Convention right must meet if a violation is to be avoided."

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]).

81. In *S v. United Kingdom* (above), the Grand Chamber concluded, in the context of proceedings challenging the legality of arrangements for the retention and

use of fingerprints and DNA, that it was necessary for there to be, among other safeguards, "detailed rules governing the scope and application of measures" so as to provide sufficient guarantees against the risk of abuse and arbitrariness (at [99]). The Court went on to state that (emphasis added):

> "103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by art. 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any … use of personal data as may be inconsistent with the guarantees of this article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family.
>
> 104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime. However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned."

82. When assessing what is required in terms of appropriate legal framework, different types of biometric information must be evaluated on their own terms. Facial biometric information is significant because it is a unique identifier for a person. But the significance of this type of biometric data is qualitatively different from, for example, DNA. A DNA sample provides access to a very wide range of information about a person.

83. In like manner, it is relevant to recognise that AFR Locate is not a form of covert surveillance. "Covert surveillance" is defined in s.26(9)(a) of the Regulation of Investigatory Powers Act 2000 ("RIPA"), which provides "…surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place…". We emphasise the words underlined. SWP accepts that were AFR to be used covertly it would be

subject to the regime in Part II of RIPA. We are satisfied that the steps generally taken by the SWP to deploy surveillance camera systems equipped with AFR in an *overt* manner are collectively sufficient such that that the provisions of RIPA 2000 are not engaged[17]. Since AFR Locate is not a form of covert intelligence gathering tool, observations made in cases that have dealt with such situations, as to the need for steps such as prior judicial authorisation or authorisation by independent administrative authority are not apposite. It would be wrong in principle when applying the "in accordance with the law" standard to start from a premise that AFR Locate is to be seen as the equivalent of covert interception whether of specific communications, or bulk communications data.

84. In our view, there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used. What is important is to focus on the substance of the actions that use of AFR Locate entails, not simply that it involves a first-time deployment by SWP of an emerging technology. The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it. 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.

(a) Primary legislation

85. The first element in the framework is the DPA 2018 (we focus on this Act rather than the DPA 1998, only for sake of convenience). As explained by Lord Sumption in *Catt* (at [8]), the DPA 2018 embeds key safeguards which apply to all processing of all personal data – including the biometric data processed when AFR Locate is used. Part 3 of the DPA 2018 applies to processing for law enforcement purposes (and gives effect to the provisions of Directive 2016/680/EU – "the Law Enforcement Directive").

86. By section 34(3) of the DPA 2018, SWP as data controller, "must be able to demonstrate its compliance with" the six data protection principles and the two safeguarding measures set out at sections 35 – 42 of the Act. These six data protection principles are as follows:

(1) processing must be lawful and fair (section 35(1));

(2) the purposes of processing must be specified, explicit and legitimate (section 36(1));

---

[17] In particular, advertising AFR deployments on Facebook and Twitter, displaying notices on AFR-equipped police vehicles and handing out of notices to members of the public (see above).

(3) personal data processed for any of the law enforcement purposes must adequate, relevant and not excessive in relation to the purpose for which is it processed (section 37);

(4) personal data must be accurate and kept up to date; inaccurate data should, subject to the purpose for which it would otherwise be retained, be corrected or erased (section 38);

(5) personal data should be kept for no longer than is necessary (section 39(1));

(6) personal data should be processed in a secure manner (section 40).

In addition, there is a relevant safeguarding measure, namely, the controller must have an appropriate policy document (section 42).

87. The data protection principles are well-known and comprehensive. They apply to all operations which involve retention or use of personal data. The fact that they are principles of general application rather than rules specifically targeted to use of AFR Locate does not make them any the less important or relevant. It is well-recognised that the need under the ECHR for any interference with Convention rights to be regulated by law can be met by standards of general application: see and compare per Lord Sumption in *Catt*, above, at [11] – [17][18]. In this instance, the general standards in the DPA 2018 have been formulated with specific reference to regulation of the use of personal data. Moreover, section 35(3) of the DPA 2018 sets out specific conditions that must be met for "sensitive processing", which includes "processing … of biometric data for the purposes of uniquely identifying an individual". As we explain below, when addressing the Claimant's data protection claims, section 35(3) does apply to the use of AFR Locate, both for the persons on the watchlists, and the members of the public whose images are caught on CCTV and then processed. The additional conditions imposed by section 35(3) include (1) that the processing is "strictly necessary" for the law enforcement purposes prescribed at section 31 of the Act; and (2) that the processing meets "at least one of the conditions in Schedule 8". The Schedule 8 conditions are each clearly and distinctly described: *i.e.* (1)(a) necessary "for the exercise of a function conferred on a person by an enactment or rule of law" or (b) necessary "for reasons of substantial public interest" or (2) necessary "for the administration of justice". The circumstances in which AFR is used are, in this way, foreseeable.

---

18 The Claimant drew our attention to the decision of the European Court of Human Rights in *Catt v United Kingdom* (2019) (ECHR application no. 43514/15). However, in that case the Court considered it unnecessary to reach any conclusion on the "in accordance with the law" issue, and the comments that it did make (see, generally, at paragraphs 94 – 107) have no specific application to the circumstances of AFR Locate. In any event, the judgment of the Supreme Court in *Catt* is binding on us (see *Kay v Lambeth London Borough Council* [2006] 2 AC 465 per Lord Bingham at [40]-[45], Lord Nicholls at [50], Lord Hope at [62], Lord Scott at [121], Lord Walker at [177], Baroness Hale at [178] and Lord Brown at [213]).

88. 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. By section 39A(7) of the 1996 Act, chief police officers must have regard to the contents of any code issued under section 39A, when exercising any relevant function. Under the Code of Practice on the Management of Police Information, the College may (and has) issued guidance which specifies principles which govern the handling of information, and this includes any processing of personal data.

(b) Secondary legislative instruments

89. The second element in the framework is the Surveillance Camera Code of Practice. This Code was issued by the Home Secretary pursuant to section 30 of the Protection of Freedoms Act 2012 ("the 2012 Act"); it contains guidance about the use of surveillance camera systems (see, generally, section 29 of the 2012 Act). By section 33 of the 2012 Act any chief officer of police must have regard to the contents of this Code when exercising any function to which it relates; and when deciding any issue in any proceedings, a court may take account of any failure to act in accordance with the requirements of the Code. Section 34 of the 2012 Act further provides that the functions of the Surveillance Camera Commissioner include encouraging compliance with the Code and providing advice in respect of its contents.

90. The Code comprises 12 "guiding principles". These principles concern when and where surveillance cameras (such as those used as part of AFR Locate) should be used; the information to be provided to members of the public when surveillance cameras are used; the extent to which information obtained from surveillance cameras should be retained; the circumstances in which access to such information should be permitted, or use should be made of the information; and the technical standards to be required of any equipment that is used. Importantly, the Code also provides that no adverse action against any person should be taken without human intervention (see paragraph 3.2.3 of the Code).

91. The Surveillance Camera Commissioner's overall submission on the Code was that it provided 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". We agree with that submission[19].

(c) SWP's own policies

92. The third element of the framework is SWP's own policies as to the use of AFR Locate. There are three relevant policy documents: (i) SWP's Standard

---

[19] We note that in March 2019 the Surveillance Camera Commissioner issued a guidance document in exercise of his power under section 34 of the 2012 Act – "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems". This guidance does not itself give rise to any legally enforceable standard. However, it does provide additional information about how the 12 guiding principles in the Code apply to the operation of AFR systems.

Operating Procedure, (ii) SWP's Deployment Reports and (iii) SWP's Policy on Sensitive Processing. Each has been produced for the purposes of the trial of AFR Locate which has been in progress since April 2017, and which remains in progress. We accept that, as the trial progresses, it is likely that these documents will be revised to reflect knowledge and insight obtained in the trial. None is a document in final form. However, taken together, they provide additional information as to how, when and in what circumstances AFR Locate may be used. Clearly it is open to SWP, from time to time, to amend the contents of any policy document. Nevertheless, for the duration of their lives, such policy documents provide legally enforceable standards against which SWP's use of AFR Locate can be judged.

93. The most important of the three documents is the Standard Operating Procedure. We have seen "Version 12" of this document. It includes the following: (a) a statement that AFR Locate will only be used overtly; (b) an explanation of the signage to be in place when AFR Locate is deployed; (c) criteria for the compilation of watchlists and for the protection of information in watchlists; (d) a statement of the time during which information obtained from the CCTV feed can be retained; (e) explanations of the respective responsibilities of the systems operator and the intervention officers; (f) guidance on the steps to be taken when the AFR equipment indicates a face match; and (g) information about Deployment Reports.

94. Deployment Reports are the second type of policy document. These documents are created, in part, in advance of any deployment and specify the purpose of the deployment and the reasons for it; and in part are completed after a deployment has finished to record the outcomes of the deployment. The existence of this type of document reflects that, to date, SWP has used AFR Locate as part of a trial exercise. However, the fact that a Deployment Report, in advance of the deployment, records the purpose of and reasons for the deployment is a material matter for present purposes.

95. The third policy document is the SWP's policy on Sensitive Processing. This is a document required by section 35 of the DPA 2018. We refer to it in further detail below, in the context of the Claimant's data protection claims.

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.

(3) Does SWP's use of AFR Locate satisfy the four-stage test in *Bank Mellat*?

Bank Mellat test

98. 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]).

99. It is common ground that there is no issue as regards the first two criteria, namely (1) that SWP uses AFR Locate for a legitimate aim, that the legitimate aim is sufficiently important to justify interfering with the Claimant's rights under Article 8, and (2) that SWP's use of AFR Locate is rationally connected to the legitimate aim. The remaining issues are (3) whether a less intrusive measure could have been used without unacceptably compromising the objective, and (4) whether a fair balance has been struck.

100. In our view, it is appropriate when applying the third and fourth criteria in the context of the facts of this case to apply a close standard of scrutiny. As we explain below, the use of AFR Locate does entail sensitive processing of personal data of members of the public, within the meaning of section 35 of the Data Protection Act 2018. This must not be undertaken other than for cogent and robust reasons. In particular, we see no reason in this regard, to draw any distinction between the levels of protection for individual rights under the Human Rights Act 1998 and the Data Protection Act 2018.

101. 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.

Conclusions on the Claimant's specific submissions

102. We turn to deal with the Claimant's submissions on proportionality, *seriatim*. First, the Claimant submits that part of the rationale for the deployment of AFR Locate at the Motorpoint Arena was that the area had only limited CCTV footage and this could have been met by the provision of additional CCTV without an AFR facility. However, the Claimant ignores two other specific purposes behind the deployment of AFR Locate on that occasion. First, the safety of the public: the event had previously attracted disorder and some of those involved in the previous protests (who were on the watchlist) had caused criminal damage and made bomb hoax calls. Second, the detection of crime: the apprehension of suspects wanted on warrant and suspects in the South Wales area. CCTV alone could not have achieved these aims: CCTV could not have identified whether those at the event were on the watchlist.

103. Second, the Claimant submits the use of AFR Locate was not limited to those who were being sought in respect of serious crime. This argument is, with respect, misconceived. The makeup of the watchlist did not have any impact on the Claimant: the impact on him would be the same if the watchlist had been limited to those sought in respect of serious crime. In fact, by including

all those who were wanted on warrant there was, potentially, a considerable additional benefit to the public interest, without any impact on the Claimant.

104. Third, the Claimant submits that SWP's use of AFR Locate is 'untargeted and speculative'. In our view, the opposite is the case, on the evidence before us. The watchlists are clearly targeted: being directed only to those people who need to be located for good reason, *i.e.* they are suspected of involvement in crimes. The choice of location is not speculative: there is good reason for considering that some of those on the watchlist may be at the locations where AFR Locate is deployed. First, those on the watchlist are, generally, those who are wanted by SWP (for offences committed in the South Wales area, or for warrants issued by South Wales courts). AFR Locate has not been used generally in support of warrants issued/offences committed elsewhere in Wales or elsewhere in the United Kingdom. Second, there are sometimes much closer connections between those on the watchlist and the particular location where AFR is deployed (as with the bomb hoaxer at the Motorpoint Arena). Third, the results speak for themselves: at most events, at least one person on the watchlist has been identified, often resulting in the apprehension of people who were wanted and would not otherwise have been identified (see above generally).

105. Fourth, the Claimant submits that AFR Locate is being used to locate people who are not suspected of having committed (or being about to commit) criminal offences. However, the vast majority of those on watchlists were those who are wanted on warrant or on suspicion of having already committed an offence. Where others are also included (*e.g.* the bomb hoaxer) then these have to be justified on a case-by-case basis. The inclusion of any person on any watchlist and the consequent processing of that person's personal data without sufficient reason would most likely amount to an unlawful interference with their own Article 8 rights.

106. Fifth, the Claimant submits that there is no evidence of a relevant change to SWP's capacity to locate criminals since AFR Locate was used. However, the evidence demonstrates that, during the present trial period, this new technology has resulted in arrests or disposals in 37 cases where the individual in question had not been capable of location by existing methods. The technology also clearly has considerable benefits in terms of saving resources that are currently deployed in searching for individuals, resources which in the future could otherwise be deployed in other ways to prevent crime and protect the public (see the evidence of Inspector Lloyd).

Further observations

107. Finally, it is noteworthy that SWP's use of AFR Locate has been the subject of independent academic analysis by Cardiff University's Police Science Institute. The UPSI Report makes it clear that AFR Locate is not a "silver bullet" and that there are a number of challenges. Nevertheless, it concluded that "The evidence clearly supports the conclusion that AFR processes and systems can contribute to police identifying persons of interest that they would not otherwise have been able to do so." It also considered that some of the

results were "impressive" and that the introduction of a new algorithm had introduced a step-change in terms of what could be accomplished.

108. Although the Claimant seeks to contend that any future use of AFR Locate would be unlawful, there is a limit to what can sensibly be said in respect of possible future use of AFR Locate by SWP. Questions of proportionality are generally fact sensitive. For present purposes, it is sufficient for us to say that, on the evidence before us as to the manner in which AFR Locate is currently deployed by SWP, we are satisfied that there is no systemic or clear 'proportionality deficit' such that it can be said that future use of AFR Locate by the SWP would be inevitably disproportionate. It will, of course, be open to any person who considers that their Article 8(1) rights have been the subject of interference because of the use of AFR Locate by SWP (or other law enforcement agency) to call on SWP to demonstrate that the interference was justified on the particular facts of the case. In this regard, it should be noted that the Information Commissioner and Surveillance Camera Commissioner have wide powers of oversight (and, in the case of the former, enforcement).

F. THE DATA PROTECTION CLAIMS

Introduction

109. The Claimant brings data protection claims under both the DPA 1998 and the DPA 2018. The two occasions in respect of which the Claimant claims SWP deployed AFR Locate when he was present (namely, December 2017 in Queen's Street and March 2018 at the Motorpoint Arena) were both before the enactment and commencement of the DPA 2018 (23rd May 2018 and 25th May 2018, respectively). In fact, none of the deployments by SWP of AFR in issue in these proceedings took place after the commencement of the DPA 2018. Nevertheless, all parties have requested that we consider the legality of the deployments of AFR Locate *as if* they had taken place after 25th May 2018. We are content to do so. SWP's pragmatic concession that the Claimant was one of the persons whose image was captured by AFR Locate at Queen's Street and at the Motorpoint Arena extends to the data protection claims. We address the data protection claims under three headings: (1) the claim under the DPA 1998; (2) the claim under section 34 of the DPA 2018; and (3) the claim under section 64 of the DPA 2018.

(1) Claim under the DPA 1998

110. The premise for the claim under the DPA 1998 is the obligation at s. 4(4) of the Act on data controllers "to comply with the data protection principles in relation to all personal data with respect to which he is the data controller". The data protection principles are at Part 1 of Schedule 1 to the DPA 1998. The first principle is that

> "personal data shall be processed fairly and lawfully and in particular, shall not be processed unless -

(a) at least one of the conditions in schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met"

111. The primary point of dispute is the extent to which using AFR Locate entails processing personal data. Three definitions at Section 1 of the DPA 1998 are relevant: *"data"*; *"processing"*; and *"personal data"*. So far as material, the definition of *"data"* is as follows

> "data means information which –
>
> (a) is being processed by means of equipment operating automatically in response to instructions giving for that purpose,
> (b) is recorded with the intention that it should be processed by means of such equipment."

"*Processing"* is defined as follows:

> "in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
>
> (a) organisation, adaptation or alteration of the information or data,
> (b) retrieval, consultation or use of the information or data, disclosure of the information or data by transmission, dissemination or otherwise making available, or
> (c) alignment, combination, blocking, erasure, or destruction of the information or data".

"Personal data" is defined as meaning

> "… data which relates 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 procession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

112. SWP accepts that the use of AFR Locate entails the processing of personal data as those terms are defined in the DPA 1998. However, it contends that the only personal data processed is the data of persons on the watchlist, since it is only those persons that SWP can identify by name. The position is

different, says SWP, in respect to those such as the Claimant whose images are captured and processed by the AFR equipment with a view to finding a match with any of the images on the watchlist. SWP could not and does not attempt to identify any of those persons (save where there is a match with a watchlist face). Thus, the information about them is not personal data.

113. Starting from the definition of personal data in the DPA 1998, it is apparent that the scope of information that is personal data is not limited simply to information about persons whom a data controller has identified by name. The definition is formulated in wider terms as to whether a person *"can be identified"* either from the data in issue, or from that data and other information held by the data controller, or from that data and other information likely to come into the data controller's possession. Thus, the definition in the DPA 1998 reflects the definition in Directive 95/46/EC ("the 1995 Directive") at Article 2 (a), which is as follows

> "personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

114. Extracting from that definition the matters particularly pertinent to the case before us, we can see no distinction between the definition in the DPA 1998 and the notion in the 1995 Directive that an "identifiable natural person" is one who "… can be identified directly or indirectly… by reference to…factors specific to his physical … identity".

115. In our view, there are two possible routes that merit examination in order to determine whether the data in issue in this case can be considered "personal data": (a) indirect identification and (b) individuation.

Indirect identification

116. The first route is indirect identification – if the data obtained by SWP through the use of AFR Locate does not itself qualify as personal data, does SWP now have, or might it in future obtain other information which when taken together with the information obtained from AFR Locate, be sufficient to render the latter personal data?

117. In its judgment in *Breyer v Bundesrepublik Deutschland* (Case C-582/14) which concerned whether dynamic IP addresses were personal data within the definition in the 1995 Directive, the CJEU took an expansive approach to indirect identification.

"40. In that connection, it is clear from the wording of Article 2(a) of Directive 95/46 that an identifiable person is one who can be identified, directly or indirectly.

41. The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.

42. Furthermore, recital 26 of Directive 95/46 states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

…

45. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject.

46. Thus … that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.

47. Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber-attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.

48. Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.

49. Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that

> provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."

118. Thus, the only incidents excluded were where the risk of identification "appears in reality to be insignificant".

Individuation

119. The second possible route is to the effect that a person is sufficiently identified for the purpose of the definition of personal data if the data 'individuates' that person.

120. In *Vidal-Hall v Google Inc.* [2016] QB 1003, in the context of an application for permission to serve proceedings out of the jurisdiction, the Court of Appeal had to consider whether it was arguable that browser generated information ("BGI") (*i.e.* information about the claimants' internet usage), was personal data. The defendant contended that the BGI was anonymous in that it neither named nor identified any person. At paragraph 115 of its judgment the court rejected that submission:

> "115. We think the case that the BGI constitutes personal data under section 1(1)(a) of the 1998 Act is clearly arguable: it is supported by the terms of the Directive, as explained in the working party's opinion, and the decision of the Court of Justice in the Lindqvist case (Case C-101/01) [2004] QB 1014. The various points made by Mr White in response do not alter our view. The case for the claimants in more detail is this. If section 1 of the 1998 Act is appropriately defined in line with the provisions and aims of the Directive, identification for the purposes of data protection is about data that "individuates" the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user. The BGI singles them out and therefore directly identifies them for the purposes of section 1(1)(a) having regard to the following: (i) BGI information comprises two relevant elements: (a) detailed browsing histories comprising a number of elements such as the website visited, and dates and times when websites are visited; and (b) information derived from use of the "double-click" cookie, which amounts to a unique identifier, enabling the browsing histories to be linked to an individual device/user; and the defendant to recognise when and where the user is online, so advertisements can be targeted at them, based

> on an analysis of their browsing history. (ii) Taking those two elements together, the BGI enables the defendant to single out users because it tells the defendant (a) the unique ISP address of the device the user is using ie a virtual postal address; (b) what websites the user is visiting; (c) when the user is visiting them; (d) and, if geo-location is possible, the location of the user when they are visiting the website; (e) the browser's complete browsing history; (f) when the user is online undertaking browser activities. The defendant therefore not only knows the user's (virtual) address; it knows when the user is at his or her (virtual) home." (emphasis added)

Thus, the court concluded that it was arguable that the BGI on its own was sufficient to identify the claimants for the purposes of the personal data definition. There was no conclusive determination of that issue in those proceedings as the claims were compromised.

121. The decision of the CJEU in *Rynes v Urad* [2015] 1 WLR 2607 is also relevant on this point. The question referred to the court in that case was whether, when a householder put up a surveillance camera to protect his property, and the camera recorded the entrance to his home, part of a public footpath, and the entrance to the house opposite, that entailed "processing of personal data … by a natural person in the course of a purely personal or household activity" and therefore was data processing outside the scope of the 1995 Directive. In the course of deciding that issue the court clearly took the view, as a necessary part of its reasoning, that the surveillance camera images comprised personal data.

> "21. The term "personal data" as used in that provision covers, according to the definition under article 2(a) of Directive 95/46, "any information relating to an identified or identifiable natural person", an identifiable person being "one who can be identified, directly or indirectly, in particular by reference … to one or more factors specific to his physical … identity".
>
> 22. Accordingly, the image of a person recorded by a camera constitutes personal data within the meaning of article 2(a) of Directive 95/46 in as much as it makes it possible to identify the person concerned.
>
> 23. As regards the "processing of personal data", it should be noted that article 2(b) of Directive 95/46 defines this as "any operation or set of operations which is performed on personal data … such as collection, recording … storage".
>
> 24. As can be seen, in particular, from recitals (15) and (16) to Directive 95/46, video surveillance falls, in principle,

> within the scope of that Directive in so far as it constitutes automatic processing.
>
> 25. Surveillance in the form of a video recording of persons, as in the case before the referring court, which is stored on a continuous recording device—the hard disk drive—constitutes, pursuant to article 3(1) of Directive 95/46, the automatic processing of personal data."

Discussion

122. In our view, the Claimant succeeds on his argument that the processing of his image by the AFR Locate equipment was processing of his personal data not on the first route but on the second. He succeeds on the basis that the information recorded by AFR Locate individuates him from all others, *i.e.* it singles him out and distinguishes him from all others.

123. On the evidence before us, the first route - the possibility of indirect identification by reference to further information that may already be or in future come to be in SWP possession - is somewhat speculative. There is nothing in the evidence in this case that is equivalent to the mechanism relied on by the court in *Breyer*, namely the ability to contact the service provider (see at paragraph 47 of the judgment in that case), and in any event, in the circumstances of the present case, this route seems artificial and unnecessary.

124. As regards the second route – individuation – in our view, the members of the public caught on the CCTV cameras are sufficiently individuated because the AFR Locate equipment takes images of their faces, that information is processed to extract biometric facial data, which is itself processed by being compared with information being drawn from the watchlist. By its nature, the facial biometric data is information about a natural person. That person is identifiable in the sense required by the definition in the 1995 Directive and the DPA 1998 because the biometric facial data is used to distinguish that person from any other person so that the matching process can take place.

125. Where the data in issue is biometric facial data, we see no need for the analysis adopted by the CJEU in *Breyer* (in the context of information comprising dynamic IP addresses). Whether or not such information is personal data may be open to debate, as is apparent from the judgment in *Vidal-Hall*. However, the biometric facial data in issue in this case is qualitatively different and clearly does comprise personal data, because, *per se*, it permits immediate identification of a person. It follows that SWP was (and is) required to process that data consistently with the data protection principles.

126. The Claimant's case that SWP acted unlawfully under section 4(4) DPA 1998 by failing to comply with the data protection principles rests only on the first data protection principle. The first requirement of that principle is that personal data must be processed lawfully and fairly. Given our conclusion on the Claimant's Article 8 claim, however, we are satisfied that the use of AFR Locate in December 2017 and March 2018 satisfied this condition of

lawfulness and fairness. On the assumption that the biometric facial data is personal data, the parties are agreed that it does not comprise *sensitive* personal data (as defined at section 2 DPA 1998). Thus, the remaining requirement under the first data protection principle is that the processing meets a Schedule 2 condition. SWP points to any of the following: (i) paragraph 3 of Schedule 2 (processing necessary for compliance with a legal obligation other than one arising from contract), (ii) paragraph 5(d) of Schedule 2 (processing necessary for the exercise of a function of a public nature, exercised in the public interest) and (iii) paragraph 6 of Schedule 2 (processing necessary for legitimate interests of the data controller, and not unwarranted by reason of interference with the data subject's rights, freedoms or legitimate interests). We consider the paragraph 6 condition to be most clearly suited to the processing in issue in this case. However, we do not rule out the application of either paragraph 3 or paragraph 5 (d).

127. Thus, and for the reasons we have set out above in the context of the Article 8 claim, the use of AFR Locate meets the requirements of the first data protection principle. The processing is necessary for SWP's legitimate interests taking account of the common law obligation to prevent and detect crime. The processing is not unwarranted for the purposes of paragraph 6, for the same reasons as it is justified for the purposes of the Article 8 claim.

(2) Claim under section 34 of the DPA 2018

128. SWP is subject to the provisions of Part 3 of the DPA 2018 on "law enforcement processing". SWP is a "competent authority" as defined in schedule 7 to the DPA 2018. Section 34 of the DPA 2018 is in Chapter 2 of Part 3 of the Act. By section 34(3), competent authorities "… must be able to demonstrate compliance with this Chapter". The remaining provisions in Chapter 2 set out the data protection principles. Section 35, which is in issue in this case, 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."

129. The Claimant's case is that the use of AFR Locate by SWP does not comply with the first data protection principle. This submission is not directed to section 35(2) of the DPA 2018 but instead to the requirements that stem from section 35(3). The Claimant contends, firstly, that AFR Locate entails *"sensitive processing"* as described at section 35(8) of the DPA 2018. SWP accepts that it does so far as it concerns processing of the biometric data of those who are on a watchlist, but disputes that the sensitive processing extends to the biometric data of members of the public whose faces are captured by the CCTV cameras. The Claimant contends, secondly, that AFR Locate does not meet the requirements of section 35(5): the processing is not *"strictly necessary"* for the law enforcement purpose; no Schedule 8 condition is met; and there is no appropriate policy document that meets the requirements of section 42(2) of the DPA 2018.

Does AFR entail processing biometric data of members of the public "for the purpose of uniquely identifying an individual"?

130. The first matter to address is the scope of sensitive processing where AFR Locate is used: does it entail processing biometric data of members of the public "for the purpose of uniquely identifying an individual"? By section 205(1) of the DPA 2018 *"biometric data"* is defined as follows.

> *"biometric data"* means 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"

131. It is beyond argument that the facial biometric data of members of the public gathered when AFR Locate is used is "biometric data" as so defined. SWP's submission is that processing this biometric data in the context of AFR Locate is not sensitive processing because the purpose of AFR Locate is not to identify the members of public *per se*, but rather to identify those on the watchlist. SWP emphasises that the necessary purpose is formulated as "the purpose of uniquely identifying an individual". This in the context of AFR Locate, says SWP, can only refer to the person on the watchlist. SWP accepts that the outcome would be different if the purpose were expressed in terms of "identifying the individual" or "identifying the individual to whom the biometric data relates", but that is not how the provision has been formulated.

132. We do not accept this submission. As a matter of straightforward language, section 35(8)(b) of the DPA 2018 can properly be read as applying both to the biometric data for those on the watchlist and to the biometric data of the members of the public. This conclusion is supported by the legislative history of the General Data Protection Regulation (Reg 2016/679/EU – "the GDPR") and the Law Enforcement Directive (2016/680/EU), measures which the DPA 2018 seek to implement. Article 9 of the GDPR lists the "special categories of

personal data". Processing of such data is prohibited unless any of ten prescribed conditions is met. One of the special categories is "biometric data [processed] for the purpose of uniquely identifying a natural person". Article 10 of the Law Enforcement Directive contains a similar form of words. From submissions made to us by the Information Commissioner, it appears that the phrase "for the purposes of uniquely identifying a natural person" was inserted during the drafting process to limit the circumstances in which processing biometric data would fall into the special category provisions of Article 9 of the GDPR and Article 10 of the Law Enforcement Directive. It is a form of words drawn from the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, as amended by a Protocol opened for signature in 2018. The Explanatory Report accompanying the Protocol included the following:

> "18. The notion of "identifiable" refers not only to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier. The use of a pseudonym or of any digital identifier/digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the Convention. The quality of the pseudonymisation techniques applied should be duly taken into account when assessing the appropriateness of safeguards implemented to mitigate the risks to data subjects
> …
>
> 58. Processing of biometric data, that is data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject.
>
> 59. The context of the processing of images is relevant to the determination of the sensitive nature of the data. The processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical means which permits the unique identification or authentication of an individual. Furthermore, where processing of images is intended to reveal racial, ethnic or health information (see the following point), such processing will be considered as processing of sensitive data.

> On the contrary, images processed by a video surveillance system solely for security reasons in a shopping area will not generally be considered as processing of sensitive data."

133. Returning to the language of section 35 of the DPA 2018, we are satisfied that the operation of AFR Locate involves the sensitive processing of the biometric data of members of the public, *i.e.* who are not on the watchlist. As described in SWP's evidence, the AFR software takes a digital image and processes it through a mathematical algorithm to produce a biometric template (*i.e.* of the member of the public who is not on the watchlist) which is then compared to other biometric templates (*i.e.* of those who are on the watchlist) in order to provide information about whether one image is like the other. That process of comparison could only take place if *each* template uniquely identifies the individual to which it relates. Although SWP's overall purpose is to identify the persons on the watchlist, in order to achieve that overall purpose, the biometric information of members of the public must also be processed so that *each* is also uniquely identified, *i.e.* in order to achieve a comparison. This is sufficient to bring processing of their biometric data within the scope of section 35(8)(b) of the DPA 2018.

134. Although the Claimant's submissions did not focus on the requirements of section 35(2) DPA 2018, the Information Commissioner made submissions as to the requirement that processing of personal data must be "*based on law"*. In substance, these submissions mirrored the matters raised by the Claimant in his *"in accordance with the law"* submission on his Article 8 claim. For the reasons we have already given on that part of the claim, we are satisfied that the *"based on law"* requirement in section 35(2) DPA 2018 is met.

Does AFR Locate meet the three requirements of section 35(5)?

135. On the basis that SWP's use of AFR Locate does entail sensitive processing does SWP's use of AFR Locate comply with the three requirements at section 35(5) of the DPA 2018? (This is the second issue summarised above at paragraph 129).

136. The first of the requirements at section 35(5) is that "the processing is strictly necessary for the law enforcement purpose". This language comes from Article 10 of the Law Enforcement Directive. In its 'November 2017 Opinion on the Law Enforcement Directive', the Article 29 Working Party (the advisory body set up under Article 29 of the 1995 Directive which comprises representatives from the Data Protection Authorities of each Member State) commented on the notion of "*strict necessity"* as follows:

> "strictly necessary … has to be understood as a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data"

In this case, the Claimant's arguments on strict necessity for this purpose comprise the matters relied on for the purposes of the proportionality submission on the claim under ECHR Article 8. For all material purposes the issue is the same. The reasons set out above at paragraphs 98 – 106 apply equally here; our conclusion is that the first of the requirements at section 35(5) of the DPA 2018 is satisfied.

137. The second section 35(5) requirement is that the processing must meet at least one of the conditions in Schedule 8 to the DPA 2018. SWP relies on paragraph 1 of Schedule 8, that

> "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".

The relevant rule of law is the common law duty to prevent and detect crime. In the context of the present claim, the 'necessity' question is addressed by the reasons we have set out above in the context of proportionality under the Article 8 claim. For these reasons, the second section 35(5) requirement is met.

138. The third section 35(5) requirement is that when the processing occurs "the controller has an appropriate policy document in place (see section 42)". Section 42(2) states the following.

> "(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."

139. SWP relies on its policy document entitled "Policy on Sensitive Processing for Law Enforcement Purposes" dated November 2018 ("the November 2018

Policy Document").[20] Although this document provides some explanation of SWP's policies for securing compliance (as required by section 42(2)), the narrative is brief and lacking in detail. We note that there is no systematic identification of the relevant policies and no systematic statement of what those policies provide. In particular, the document does not appear to address the position of members of the public. For these reasons, we think it is open to question whether this document, as currently drafted, fully meets the standard required by section 42(2).

140. It is right to observe that the description of the appropriate document in section 42(2) DPA 2018 is itself generic. We note that, when referring to the section 42 "appropriate policy", the Information Commissioner's website does no more than set out what the Act says. 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. In her Skeleton Argument for this hearing, the Information Commissioner suggested that "ideally" the SWP document should be more detailed. We agree.

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.

(3) Claim under section 64 of the DPA 2018

142. Section 64 of the DPA 2018 sets out an obligation to undertake impact assessments.

> **"64 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.

---

[20] The full title is "Policy on Sensitive Processing for Law Enforcement Purposes under Part 3 Data Protection Act 2018. South Wales Police (SWP) Automated Facial Recognition (AFR). Processing biometric data to uniquely identify a person" dated November 2018 ("the November 2018 Policy Document").

> (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."

143. SWP prepared an impact assessment in respect of its use of AFR equipment. We have seen *Version 5.4*, dated 11th October 2018. The Claimant contends this assessment is defective: (a) because it is not written on the premise that use of AFR Locate entails sensitive processing of personal data of members of the public; and (b) because it does not recognise the interference with Article 8(1) rights of those members of the public. The Claimant also complains that no data protection impact assessment was in place as at 25th May 2018, the commencement date of section 64 of DPA 2018.

144. This latter point is not a matter of any substance. SWP's evidence was that prior to May 2018 it had undertaken what it describes as a "Privacy Impact Assessment". We have seen *Version 4* of that document, dated 12th February 2018. Among other matters, that document included consideration of the data protection consequences of AFR Locate. SWP's evidence is that, following commencement of the DPA 2018, the Privacy Impact Assessment was revised and retitled as a "Data Protection Impact Assessment". Thus, we are satisfied that at all material times the processing by SWP was supported by a relevant impact assessment.

145. The obligation of a data controller under section 64 of the DPA 2018 is to undertake an assessment of the possible impact of the proposed processing of personal data, and as part of that assessment: (a) to describe the processing operations; assess the risks arising from those operations to the rights of data subjects; (b) to identify any measures it proposes to take to address those risks; and (c) to identify any measures it proposes to put in place as safeguards to help ensure protection of personal data. Where the issue is whether a data controller has complied with the section 64 obligation, the approach required of the Court - or for that matter of the Information Commissioner should the

matter come before her through the enforcement provisions under Part 6 of and Schedule 13 to the DPA 2018 - is not dissimilar to the approach courts already take when considering claims of failures to comply with the public-sector equality duty under section 149(1) of the Equality Act 2010. Although the respective obligations are not identical, both require prior consideration of matters relevant to a proposed course of conduct, and an exercise of judgement on the part of the decision-maker as to the steps that should be taken to guard against possible adverse consequences of the action proposed.

146. On a complaint about a failure to comply with section 64 DPA 2018, it is for the Court to decide whether the data controller has discharged that obligation. What is required is compliance itself, *i.e.* not simply an attempt to comply that falls within a range of reasonable conduct. However, when determining whether the steps taken by the data controller meet the requirements of section 64, the Court will not necessarily substitute its own view for that of the data controller on all matters. The notion of an assessment brings with it a requirement to exercise reasonable judgement based on reasonable enquiry and consideration. If it is apparent that a data controller has approached its task on a footing that is demonstrably false, or in a manner that is clearly lacking, then the conclusion should be that there has been a failure to meet section 64 obligation. However, when conscientious assessment has been brought to bear, any attempt by a court to second-guess that assessment will overstep the mark. In the context of the public-sector equality duty, in his judgment in *R (Unison) v Lord Chancellor* [2016] ICR 1, Underhill LJ made this observation, at paragraph 106:

> "… to the extent that views are expressed on matters requiring assessment or evaluation the court should go no further in its review than to identify whether the essential questions have been conscientiously considered and that any conclusions reached are not irrational. Inessential errors or misjudgements cannot constitute evidence of the breach of the duty."

147. In our view, a like approach is required for the purposes of the impact assessment obligation under section 64 DPA 2018. When considering whether or not a data controller has complied with the section 64 obligation, a Court will have regard to the guidance that has been issued by the Information Commissioner in respect of Data Protection Impact Assessments. However, it is important to have well in mind that that guidance is non-statutory, *i.e.* it is not issued under the auspices of section 127 DPA 2018. Weight should, of course, attach to opinions expressed by the Information Commissioner in her guidance, but they should not cause anyone to lose sight of either (a) the obligations in section 64 as they have been expressly formulated, or (b) the appropriate standard of review of a data controller's impact assessment exercise.

148. We consider that the impact assessment prepared by SWP in this case meets the requirement of section 64 DPA 2018. There is a clear narrative that explains the proposed processing. This refers to the concerns raised in respect of intrusions into privacy of members of the public when AFR Locate is used.

Although it is no part of the requirements of section 64 that an impact assessment identifies the legal risks arising from the proposed processing, the SWP's assessment specifically considers the potential for breach of Article 8 rights. The Claimant's criticism on this point is therefore without foundation. Nor do we accept the Claimant's other criticism of the Data Protection Impact Assessment Document. It is correct that the treatment of the personal data of those on watchlists is a particular focus of the document. However, the document does recognise that personal data of members of the public will be processed, and identifies the safeguards that are in place in terms of the duration for which any such data will be retained, the purpose for which it will be used, and so on. See for example at pages 19 to 22 of the document.

G. THE PUBLIC-SECTOR EQUALITY DUTY CLAIM

Introduction

149. SWP first sought funding for its trial of AFR Locate in January 2017. By April 2017, SWP had in place both funding, and an agreement with NEC for use of its automatic facial recognition software application, NeoFace Watch.

150. By section 149(1) of the Equality Act 2010, public authorities must in the exercise of their functions have due regard to three matters: (a) the need to eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the 2010 Act; (b) the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and (c) the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it. What those criteria require is further explained in the remainder of section 149.

151. In April 2017, SWP prepared a document titled *"Equality Impact Assessment - Initial Assessment"*. It relies on this as evidence of its compliance with the section 149(1) duty. The fact that the document is described as an *"Initial Assessment"* is immaterial. It is well-established that public authorities should seek to consider the section 149(1) criteria at the earliest realistic stage of a decision-making process. In this instance, as at April 2017 SWP was commencing a trial of AFR technology. It was entirely appropriate for SWP to undertake early assessment of the possible consequences in section 149 terms of that trial leaving open the possibility of further evaluation by reference to the section 149(1) criteria as the project developed.

152. The Claimant's criticism of SWP is that 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 false positive matches for female faces and/or for black and minority ethnic faces. Thus, contends the Claimant, due regard was not had either to the need to eliminate discrimination or the need to foster good relations.

Discussion

153. In our view, and 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 licenced might operate in a way that was indirectly discriminatory. Indeed, even now there is no firm evidence that the software does produce results that suggest indirect discrimination. 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.

154. In a statement dated 26th November 2018 made on behalf of SWP, Dominic Edgell an officer in the SWP's Digital Services Division provided information about the rate of false positive matches based on deployments of AFR Locate between May 2017 and June 2018. That was that the rate of false positives was proportionally higher for men than women; and that the proportion of female false positive alerts compared to the total number of female alerts was higher than the proportion of male false positive alerts to the total number of male alerts. When Mr. Edgell investigated this, he concluded that the higher proportion of female false positives was the consequence of two watchlist female faces which had significant generic features. His evidence is that the variation was because these specific faces were on the watchlists, not the consequence of gender bias. Mr. Edgell also explained that he reviewed the use of AFR Locate for bias based on ethnic origin. His results suggested no such bias.

155. In a second statement dated 25th January 2019 Dr Jain commented as follows on AFR Locate (at paragraph 15):

> "I cannot comment on whether AFR Locate has a discriminatory impact as I do not have access to the data sets on which the system is trained and therefore cannot analyse the biases in those data sets. For the same reason, the defendant is not in a position to evaluate the discriminatory impact of AFR Locate. However, bias has been found to be a feature of common AFR systems."

and then on Mr. Edgell's evidence (at paragraphs 34 to 35)

> "34. Mr. Edgell concludes that he has seen no gender bias when using AFR technology. Despite there being proportionally more false positive female alerts than false positive male alerts, he explains this as being due to the presence of two "lambs" …

> 35. Before it is possible to draw conclusions on the existence of gender bias, an extensive study needs to be conducted where match scores are thoroughly analysed for both males and females, regardless of whether they generate alerts or not. Mr. Edgell does not carry out this study; he considers only alert statistics."

("Lambs" is a label used by the software providers to describe faces that have a number of common generic features such that more frequent matches are generated by the facial recognition software.)

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.

H. CONCLUSION

159. For the reasons set out above, the Claimant's claim for judicial review is dismissed on all grounds. We are satisfied both that the current legal regime is

adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that SWP's use to date of AFR Locate has been consistent with the requirements of the Human Rights Act, and the data protection legislation.

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[21]:

   (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.

[21] Similar principles are now to be found in Part 3 of the DPA 2018 (see below).

(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 Protection of Freedoms Act 2012 ("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 SC Code.

11. Section 30 provides that the Secretary of State must lay the code of practice and order providing 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. 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 ("the SC Code of Practice") (see further below).

Data Protection Law Enforcement Directive (2016/680/EU) ("the Law Enforcement directive")

18. The Law Enforcement Directive came into force on 6 May 2018. Its purpose includes to further the right to protection of personal data under Article 8(1) of the Charter of Fundamental Rights of the European Union (see the first recital). By Article 3(13) biometric data is defined to mean personal data resulting from specific technical processing relating (amongst other matters) to:

> "the physical… characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images...".

19. Article 10 permits the processing of biometric data for the purpose of uniquely identifying a natural person, unless it is both (a) strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject; and (b) either authorised by State law, to protect the vital interests of the data subject or of another natural person, or where it relates to data manifestly made public by the data subject.

Data Protection Act 2018 ("DPA 2018")

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

21. 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. …

22. 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."

23. 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."

24. Section 35 reflects the language and scope of Article 10 of the Law Enforcement Directive.

> "*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

25. 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".

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

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

27. 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

28. 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).

29. 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)…"

30. 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."

Code and Guidance

Secretary of State's Surveillance Camera Code of Practice

31. 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."

32. The Code of Practice 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.

33. Relevant paragraphs from the SC Code are as follows:

> "1.8 This code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places."

> "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

34. 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 IC 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 Code of Practice (paragraph 1.3).[22]

35. 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" (Code of Practice, 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).

36. 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.

[22] It is assumed that this reference in paragraph 3.1 of the SCC AFR Guidance was intended to be to s.33 because s.31(1) concerns the Secretary of State keeping the Code of Practice under review.

37. 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 Claimant complains).

The Information Commissioner

38. The Information Commissioner published high level guidance on the safeguards for law enforcement processing under Part 3 of the DPA 2018, and in particular as the appropriate policy to be issued:

> "**What safeguards are required for sensitive processing?**
>
> If you are carrying out sensitive processing based on the consent of a data subject, or based on another specific condition in Schedule 8 of the Act, you must have an appropriate policy document in place.
>
> The appropriate policy must explain:
>
> - your procedures for complying with the data protection principles when relying on a condition from Schedule 8; and
>
> - your policy for the retention and erasure of personal data for this specific processing.
>
> You must retain this policy from the time you begin sensitive processing until six months after it has ended. You must review and update it where appropriate and make it available to the Information Commissioner upon request without charge."

39. The Information Commissioner states that, whilst further clarification and detail is required (particularly in relation to the specific Schedule 8 condition relied on for AFR, and on lawfulness and fairness), she is of the view that the SWP's current document does meet the requirements to constitute an overarching "appropriate policy document" within s.42 of the DPA 2018. We agree.

SWP Documents

SWP Policy Document

40. 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 Policy Document"). The Policy Document sets out SWP's policy as regards compliance with the six Data Protection Principles in Part 3 of the PDA 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")

41. SWP has Automatic Facial Recognition Standard Operating Procedures ("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 watch lists should be "proportionate and necessary" for each deployment and primary factors for the inclusion on watch lists 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

42. 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 Chief's Council.