LIBERTY
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty House
26–30 Strutton Ground
London SW1P 2HR

TELEPHONE 020 7403 3888
FACSIMILE 020 7799 5306

DIRECTOR
Martha Spurrier

LEGAL OFFICERS
Emma Norton, Head of Legal Casework
Rosie Brighouse, Solicitor
Debaleena Dasgupta, Solicitor
Lara ten Caten, Solicitor

Mr Matt Jukes
Chief Constable of South Wales Police
South Wales Police Headquarters
Cowbridge Road
Bridgend
CF31 3SU

ACPO.Staff.Office@south-wales.pnn.police.uk

11 June 2018

By email and by post

LETTER BEFORE CLAIM

Dear Mr Jukes

Proposed judicial review of South Wales Police's use of automated facial recognition technology

1. I act for Mr Edward Bridges. I write pursuant to the Pre-Action Protocol for Judicial Review to inform you that my client proposes to make an application for judicial review challenging the lawfulness of the ongoing use of automated facial recognition ("**AFR**") technology by South Wales Police ("**SWP**").

2. In bringing this claim Mr Bridges relies on and seeks damages for the violation of his rights under the European Convention on Human Rights ("**ECHR**") and the Data Protection Act 1998 ("**DPA 1998**") in respect of two instances of SWP using AFR technology against him on 21 December 2017 and 27 March 2018. Given the relationship between these instances of AFR use (in respect of which there are unlikely to be any significant factual disputes) and my client's challenge to SWP's ongoing deployment of this technology in the area in which he resides, it would clearly be efficient and proportionate to address these matters and his damages claim as part of the proposed claim for judicial review.

Proposed Claimant

3. The proposed claimant is Mr Edward Bridges of 15 Quentin Street, Gabalfa, Cardiff CF14 3JW. He is a man of good character, with no previous arrests, cautions or convictions.

4. Mr Bridges seeks to challenge SWP's use of AFR technology as a concerned resident of the SWP police area who, it can be inferred, has already been subjected to the technology and who, as a resident of and regular user of public spaces in the police area, may in the future be the subject of SWP's use of AFR technology.

Proposed Defendant

5. The proposed defendant is the Chief Constable of SWP.

6. I also consider that the Home Office, as the central government department responsible for policing, is an Interested Party and will be named as such. If you do not agree, please set out your reasons.

Decision under challenge

7. The ongoing decision of SWP to use AFR technology in public places within the SWP police area.

Funding

8. My client intends to fund his proposed claim by way of crowdfunding. He also intends, if and when permission is granted, to apply for a Costs Capping Order ("**CCO**") under sections 88 to 90 of the Criminal Justice and Courts Act 2015 to cap his contingent costs liability at such amount that it has been possible to raise through crowdfunding. Evidence as to our client's financial position will be provided at the appropriate juncture and to the extent that this matter cannot be resolved without recourse to litigation. At this stage it suffices to say that the criteria for a CCO would plainly be satisfied. The proposed claim raises issues of significant general public importance including on the basis that the number of people affected by SWP's use of AFR technology is substantial, the extent of the intrusion into ECHR rights entailed by this technology and the fact that points of law of general public importance arise. Should litigation prove necessary, our client is open to seeking to agree an appropriate costs cap and we would welcome any proposals as to the same.

Background to the claim

9. The background to this claim is set out on the basis of the facts as they are known to my client through information available in the public domain. To the extent that this summary of the factual position is incorrect, we ask that you clarify the position and provide all relevant documentation in support of any such corrections. Otherwise, my client shall be entitled to proceed on the basis of the facts as they are set out in this letter.

<u>AFR technology</u>

10. AFR technology works to scan in real time the faces of all passers-by within range of an AFR camera. The software measures the biometric facial characteristics of each person scanned in order to create a unique facial map in the form of a numerical code which is then, through the use of algorithms, compared with other facial images held by police in order to find a match. This may be done in real time or after the event and functions through the use of video footage as well as still images. The technology does not require any physical contact or human engagement with it in order to function, and the people being scanned by the technology do not need to provide consent at any stage; they may not even be aware that the technology is in use.

11. The (mis)use of AFR technology by police forces involves and/or is contingent on at least six discrete, yet related, activities which involve the use of personal data and/or other

interferences with the rights of individuals:

a) the obtaining of visual information concerning individuals through measures unrelated to the use of AFR technology (**"the control data"**);

b) the storage in electronic systems of the control data;

c) the taking of video footage and/or still photographs of persons by AFR cameras (**"the surveillance data"**);

d) the retention/storage of the surveillance data;

e) the processing of the surveillance data through automated referencing against the control data with a view to identifying individuals of interest; and

f) the taking of enforcement action on the basis of such identification.

12. This claim focuses on the use of AFR technology as summarised in (c) – (e) above.

Inadequate legal basis, oversight, policy or guidance

13. The Government has stated "*There is no legislation regulating the use of CCTV cameras with facial recognition*".[1] The Government has pointed to the Surveillance Camera Code of Practice 2013 ("**COP 2013**"), noting that it requires police use of AFR technology to be clearly justified and proportionate.[2] The COP 2013 is not legally binding and does not specifically deal with the use of AFR technology, beyond requiring justification and proportionality. The lack of an adequate legislative framework on AFR technology has been criticised by the Biometrics Commissioner, who has argued that such a framework is "*urgently needed*".[3]

14. The Government has stated that "*A decision to deploy facial recognition systems is an operational one for the police.*"[4] This approach has been criticised by the House of Commons Science and Technology Committee, which recommended that decisions on the future deployment of AFR technology be made by Government and Parliament rather than be left to be an operational police matter.[5] The Government's Biometrics Strategy, which is four and a half years overdue, is yet to be published and no independent oversight body has been appointed to review the use of AFR technology – something that the Surveillance Camera Commissioner has expressed concern about.[6] As a result

---

1 Written parliamentary question answered by Mr Nick Hurd MP on 12 September 2017, available here: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/.

2 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/.

3 https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

4 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/171130-BWT-to-Chair-biometric-strategy.pdf.

5 'Biometrics strategy and forensic services: Fifth report of session 2017-19', 23 May 2018, paragraph 50, available here: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf.

6 'Review of the impact and operation of the Surveillance Camera Code of Practice', February 2016, p.15, available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502893/Draft_Review_FINAL.pdf.

– and as the Surveillance Camera Commissioner also notes[7] – it is police forces who are the ones developing governance on the use of AFR technology. The Information Commissioner has also expressed her concern "*about the absence of national level co-ordination in assessing the privacy risks and a comprehensive governance framework to oversee [AFR technology] deployment.*"[8]

15. For present purposes, the absence of guidance at the national level places an increased burden on individual police forces that choose to use AFR technology to ensure that they do so in a lawful manner. Whilst a breach of the COP 2013 does not give rise to automatic civil or public law liability, SWP, like all other public authorities using surveillance cameras, is obliged to take it into account, and any failure to adhere to it will be highly relevant when considering the lawfulness of any steps taken. The COP 2013 mandates systems operators to adopt the following guiding principles:[9]

> *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.*

---

7 https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

8 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/.

9 Paragraph 2.6 of the COP 2013, available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

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.

16. On the information presently available, SWP is or may be in breach of at least principles 1, 2, 3, 8 and 10, as referenced where appropriate below.

Inaccuracy and discrimination

17. In addition to there being no adequate legislative framework or governance structure, AFR technology has also been shown to be inaccurate and discriminatory and thus ineffective in achieving its law enforcement aims.

18. Information in the public domain indicates that SWP has arrested only 15 people as a result of their being identified through the use of AFR technology; 2,451 people have been wrongly identified, 31 of whom were requested by the police to confirm their identity.[10]

19. The publicly available evidence shows that AFR technology disproportionately misidentifies female and black and ethnic minority ("**BME**") faces. This results from a problem in the development of artificial intelligence systems, namely the lack of diversity of people and opinions in databases used to 'train' these systems. In the case of AFR technology, studies in the US have shown that this has resulted in higher error rates in relation to the identification of women and BME people.[11] Given that the datasets used to train algorithms in AFR software used by UK police forces (including SWP) are likely to be similarly biased, the same problem will occur in relation to UK use of AFR technology – women and BME people will be disproportionately misidentified and thus impacted by use of the technology. This discriminatory impact is another aspect of the use of AFR technology that the Surveillance Camera Commissioner has criticised.[12]

20. It is also of note that guiding principle 8 of the COP 2013 specifically requires that any use of AFR technology is done in accordance with operational and technical standards relevant to that system and for its stated purpose. If, as seems highly probable, the operational standards for AFR Locate (the AFR system SWP uses) require it to have a sufficiently broad and representative dataset in order to be accurate, then an inadequate dataset would be in breach of that and in turn in breach of guiding principle 8.

SWP's use of AFR technology

21. SWP has been at the forefront of the deployment of AFR technology in the UK. In

---

10 https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Revised-response-286_18.pdf.

11 Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', in *Proceedings of Machine Learning Research* 81:1, 2018, available here: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; and Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge and Anil K. Jain, 'Face Recognition Performance: Role of Demographic Information', in *IEEE Transactions on Information Forensics and Security*, available here: http://openbiometrics.org/publications/klare2012demographics.pdf.

12 https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

partnership with technology company NEC, it uses an AFR system named 'AFR Locate'.[13] SWP has benefitted from government funding in order to trial and use AFR technology – £1.2m in 2016/17 and £0.8m in 2017/18 from the Home Office, and £0.6m from Home Office Biometrics. SWP has also contributed £100,000.

22. SWP first used AFR technology in a live public environment in May/June 2017 in the run up to and at the UEFA Champions League final in Cardiff.[14] Since then, it has used the technology in live public environments at least 20 more times, and (despite the fact that its contract to 'trial' the technology has ended)[15] is due to use it again later this month (June 2018).[16] For most of these deployments, SWP used the technology in relation to a specific event. However, on several of those occasions SWP used the technology in locations in Cardiff city centre in addition to at the event itself.[17]

23. Further, SWP has used AFR technology on days when there has been no specific event to police. For example, AFR technology was used in Cardiff city centre on 18 October 2017 and 21 December 2017,[18] and as part of its 'Operation Fulcrum' on 19 October 2017 and 22 December 2017 and 'Operation Malecite' on 23 December 2017.[19] My client witnessed first-hand SWP use AFR technology on Queen Street – a busy shopping street in Cardiff city centre – on 21 December 2017.

24. SWP has stated that it has been using AFR technology largely to target petty criminals with histories of low-level offences like pick-pocketing.[20] In addition to targeting petty criminals, however, SWP has also used AFR technology to target protestors. One event at which SWP used AFR technology was the peaceful protest outside the Defence Procurement, Research, Technology and Exportability event – commonly referred to as the Cardiff Arms Fair – which took place on 27 March 2018 at the Cardiff Motorpoint Arena. My client attended the Cardiff Arms Fair to protest peacefully and again witnessed first-hand SWP's use of AFR technology.

---

13 https://www.south-wales.police.uk/en/advice/facial-recognition-technology/.

14 https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Revised-response-286_18.pdf.

15 https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Revised-response-286_18.pdf.

16 SWP has confirmed its use of AFR technology at the following events: the Elvis Festival, the Anthony Joshua v Kubrat Pulev boxing match, seven Wales rugby matches, a Kasabian concert, a Liam Gallagher concert, a Stereophonics concert, the BBC Big Weekend music festival, a royal visit, the Cardiff Arms Fair, in relation to Operation Fulcrum (on two occasions) and Operation Malecite, and in Cardiff city centre on 18 October 2017 and 21 December 2017. It has also confirmed that it will use AFR technology at a Rolling Stones concert on 15 June 2018. See: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Revised-response-286_18.pdf; https://www.south-wales.police.uk/en/advice/facial-recognition-technology/; and https://twitter.com/inspectorslloyd?lang=en.

17 For example, SWP used AFR technology in Cardiff city centre on the days of the Anthony Joshua v Kubrat Pulev boxing fight (28/10/2017), the Wales v Australia rugby match (11/11/2017), the Wales v South Africa rugby match (2/12/2017), the Wales v Scotland rugby match (3/2/2018), and the Wales v France rugby match (17/3/2018). See Inspector Scott Lloyd's Twitter: https://twitter.com/inspectorslloyd?lang=en.

18 https://twitter.com/inspectorslloyd?lang=en.

19 https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Revised-response-286_18.pdf.

20 See, for example, SWP's press release ahead of its deployment of AFR technology at the Kasabian concert at the Motorpoint Arena in Cardiff on 4 December 2017: https://motorpointarenacardiff.co.uk/news-and-alerts/facial-recognition-technology-partnership-south-wales-police; and Inspector Scott Lloyd's Twitter in relation to the same deployment as well as a deployment on 3 February 2018: https://twitter.com/inspectorslloyd?lang=en. This conflicts with the justification contained in SWP's draft Privacy Impact Assessment for using AFR technology – that there is an "*operational imperative to deploy the technique as part of the control strategy for a high risk, high profile event*" (p.13, available here: https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf) – and the Chief Constable of SWP's personal comments in response to criticism about the number of false positives, where he relied on the potential risk of terrorism at events as a justification: https://www.bbc.co.uk/news/uk-wales-south-west-wales-44007872.

25. Images captured by AFR cameras are stored by SWP for (at least) 31 days.[21]

Proposed grounds of judicial review

26. SWP's ongoing use of and recourse to AFR technology is unlawful in that it breaches:

    a) Articles 8, 10, 11 and 14 of the ECHR;

    b) the public sector equality duty in section 149(1) of the Equality Act 2010; and

    c) the first and third data protection principles of Part 3 of the Data Protection Act 2018 ("**DPA 2018**").

27. Further, my client brings a claim for damages under the Human Rights Act 1998 ("**HRA**") for a breach of his rights under Articles 8, 10 and 11 and under the DPA 1998 (taken with the transitional provisions contained in the DPA 2018) in respect of SWP's use of AFP technology against him in Cardiff on 21 December 2017 and 27 March 2018.

Breach of Article 8 of the ECHR

28. As a public authority, SWP is under a duty imposed by section 6(1) of the HRA to respect the rights of individuals under the ECHR.

29. Article 8(1) of the ECHR provides that "*Everyone has the right to respect for his private and family life, his home and his correspondence.*" The use of AFR technology as described above at paragraphs 11 and 21 to 25 clearly engages the Article 8 rights of my client and those of any member of the public against whom the technology is or *may be* used. The capturing of images through AFR cameras, the algorithmic processing of these images alongside existing information held by SWP, and the storage of images captured through AFR cameras constitute discrete interferences with Article 8. The use of AFR technology is qualitatively different from conventional CCTV due to its processing of biometric data – such data is special category personal data under the GDPR.

30. Article 8(2) provides that the right to privacy cannot be interfered with by a public authority "*except such as is in accordance with the law and is necessary in a democratic society*". Whether the interference is necessary in a democratic society depends on whether the interference is a proportionate means of meeting a pressing social need.

31. For the reasons set out at paragraphs 13 to 14 above, the use of AFR technology has no adequate legal basis or framework and is therefore not in accordance with the law. In particular, this framework (i) does not give individuals adequate protection against arbitrary interferences with Article 8 rights, (ii) is not formulated with sufficient precision to enable individuals to regulate their conduct, and (iii) does not contain sufficient safeguards to enable the proportionality of the interferences to be adequately examined.[22] For this reason alone, SWP's use of AFR technology infringes my client's right to privacy under Article 8.

32. My client does not accept that there is any pressing social need (in a democratic society,

---

21 SWP's draft Privacy Impact Assessment, 12 February 2018, p.17, available here: https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf.

22 *R (T) v Chief Constable of Greater Manchester* [2015] AC 49; *S v UK* (2009) 48 E.H.R.R. 50.

at least) to deploy a highly invasive form of technology which entails capturing video footage of *everyone* within the camera's range of vision and further processing the biometric data of all individuals whose facial images are captured by an AFR camera.

33. Without prejudice to this position, SWP's use of AFR technology is not necessary and proportionate for at least the following reasons:

    a) AFR technology is a highly intrusive method of policing that indiscriminately scans, maps and checks the identity of each person within its range and captures personal biometric data in the process.[23] This occurs without any legal requirement that particular requirements are met in terms of the threat posed in a given area at a specific time before the technology can be deployed, less still any individualised suspicion in relation to those whose images are captured and processed. Its use may result in members of the public being stopped and questioned by the police following a match (which may or may not be accurate). The disproportionality of the technology's use is magnified by the fact that members of the public are unable to consent to its use, and many remain unaware that they have even been subjected to it.[24]

    b) A less intrusive measure could undoubtedly have been used / be used by SWP for the purposes of its legitimate policing objectives. My client relies on the fact that SWP was in a position to perform properly its functions with less intrusive policing techniques before the advent of AFR technology. The mere existence of a particular form of technology does not justify its deployment as necessary and proportionate. Further, he will rely on the fact that the Information Commissioner recently demanded that police forces provide clear evidence of the necessity and also the effectiveness of AFR technology.[25]

    c) It is well established that the justification for the use by the police of images of individuals must be more compelling where the interference with a person's rights is (as is the case in respect of SWP's use of AFR technology) in pursuit of the protection of the community from the risk of public disorder or low level crime.[26]

    d) Having regard to (i) the fact that less intrusive measures are available to pursue any legitimate aims pursued by SWP through the use of AFR technology, and (ii) the severity of the consequences for individuals' rights, it cannot sensibly be said that a fair balance has been struck between the rights of the individual and the interests of the community in the context of SWP's use of AFR technology.

34. In this context, it is deeply alarming that SWP considers AFR technology an appropriate

---

23 The Information Commissioner has expressed her concerns that use of AFR technology "*can be particularly intrusive*" in a blog post dated 14 May 2018: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/.

24 The fact that AFR technology can be used without people's cooperation is hailed as "*a significant advantage*" by SWP in its draft Privacy Impact Assessment, 12 February 2018, p.3, available here: https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf. SWP claims in its draft Assessment that there has been "*widespread publicity*" in advance of deployments of AFR technology (p.13). While there has been some publicity ahead of certain deployments (e.g. the Champions League final), other deployments, in particular in Cardiff city centre, have happened without "widespread publicity".

25 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/.

26 *R (Wood) v Commissioner of Police the Metropolis* [2010] 1 W.L.R. 123 at [86].

method of policing members of the public and peaceful protestors and has reached that view without any adequate public consultation, contrary to the COP 2013 (see for example guiding principles 2 and 3, paragraphs 3.2.4, 3.3.2 – referring to consultation as "*an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response*" – and 3.3.3).

Breach of Articles 10 and 11 of the ECHR

35. Article 10 of the ECHR provides that "*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without inference by public authority and regardless of frontiers.*" Further, Article 11 of the ECHR provides that "*Everyone has the right to freedom of peaceful assembly and to freedom of association with others….*".

36. Protestors exercise both of these rights when attending demonstrations and expressing their views in favour of a particular cause. By attending the Cardiff Arms Fair protest, my client was exercising his right to express his opinion regarding the Cardiff Arms Fair as well as his right to assemble peacefully in order to communicate that opinion.

37. SWP's use of AFR technology interferes with the exercise of these rights in two ways. Firstly, it has a chilling effect on people's attendance of public events and peaceful protests. Members of the public with concerns about their privacy, or the possibility that their identities will be checked and/or tracked by the police, are likely to be deterred from attending protests at which AFR technology is in use. My client has several friends and colleagues in this position who have explained to him that they would feel uncomfortable attending (or would not attend at all) a protest where AFR technology is in use. This suggests that the technology interferes with and dampens people's willingness to attend and participate in protests.

38. Secondly, once at a protest or event where AFR technology is being used, the presence of the AFR van itself is intimidating and is apt to interfere with people's freedom of expression. The van sends a message to members of the public that they are being watched by the technology and that they can be identified. It creates an environment where members of the public are treated as suspects and not as citizens exercising their rights to expression and association. As a result, people are less likely to voice their honest (lawful) opinions and behave in the (lawful) way they would were the AFR van not present.

39. It is clear from the points made in paragraphs 13 to 14 above that SWP's use of the technology is not prescribed by law. For the reasons detailed at paragraph 33, and in light of the chilling and intimidating effects of AFR technology, SWP's use of the technology is neither a necessary nor proportionate interference with my client's rights under Articles 10 and 11 of the ECHR.

Breach of Article 14 of the ECHR

40. Article 14 of the ECHR prohibits discrimination on, amongst other bases, the grounds of sex, race and colour in the context of the enjoyment of ECHR rights. A measure that has disproportionately prejudicial effects on a particular group may be considered

discriminatory notwithstanding that it is not specifically aimed at that group.[27]

41. SWP's use of AFR technology infringes Article 14 (taken with Articles 8, 10 and 11, for the reasons articulated above) because it discriminates against women and BME people for no objective or reasonable reason. Paragraph 19 above explains how AFR technology has been shown to disproportionately misidentify women and BME people. People with these characteristics are plainly in an analogous position to those who do not share these characteristics when subject to the use of AFR technology. When exercising their rights under Articles 8, 10 and 11, members of these groups are likely to be treated less favourably than others in the same position by virtue of their sex, race and/or colour. Such differential treatment is incapable of any objective or reasonable justification.

Breach of the public sector equality duty

42. Pursuant to section 149(1) of the Equality Act 2010, SWP is subject to the public sector equality duty ("**PSED**") – it "*must, in the exercise of its functions, have due regard to the need to...eliminate discrimination, harassment, victimisation and any other conduct that is prohibited under this Act.*" The PSED requires a public authority to be properly informed of the equality implications before taking a decision and if the relevant material is not available there will be a duty to acquire it.[28] The duty must be discharged before the relevant decision is taken/policy is adopted; it cannot be a rear-guard action,[29] and it is a duty of an ongoing nature.

43. In its draft Privacy Impact Assessment[30] on AFR technology SWP explained that complying with the PSED duty meant "*working with members of the public who reflect local diversity to ascertain any impact (whether positive or negative) that the use of such a system may have.*"[31] This is plainly insufficient to discharge the PSED. It does not appear that SWP conducted any or any adequate equality impact assessment either before AFR technology was first approved for deployment in the SWP police area or at any other time.

44. For the reasons outlined above in paragraph 19, there is evidence that AFR technology has a disproportionately negative and discriminatory impact on women and BME people. If it had complied with the PSED, SWP would not have used the technology without having rigorously tested it for (and corrected) negative biases and it would have made publicly available any documentation in which it considered the technology's discriminatory impact. No such information has been published by SWP.

---

27 *D.H. and Others v Czech Republic*, App. No. 57325/00 at [175].

28 *Bracking v Secretary of State for Work and Pensions* [2013] EWCA Civ 1345 at [28(8)]; and *R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills* [2012] EWHC 201 (Admin) per Elias LJ at [89-90].

29 *Kaur & Shah v LB Ealing* [2008] EWHC 2062 (Admin).

30 The fact that SWP's draft Privacy Impact Assessment was only published on 12 February 2018 (with no indication of when a finalised version will become available) suggests that SWP has taken a rear-guard approach to its PSED. Failure by SWP to carry out and publish a finalised Privacy Impact Assessment before first using AFR technology would indicate a breach of COP 2013 guiding principle 2.

31 SWP's draft Privacy Impact Assessment, 12 February 2018, p.10, available here: https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf.

Breaches of the Data Protection Acts 1998 and 2018

Ongoing breach of the DPA 2018

45. SWP's ongoing use of AFR technology is in breach of the DPA 2018. The processing of personal data by the police for the purpose of the prevention, investigation, detection or prosecution of criminal offences is covered by Part 3 of the DPA 2018, which is the UK's implementing legislation for EU Data Protection Directive 2016/680 (the Law Enforcement Directive).

46. Each element of SWP's use of AFR technology (as set out at paragraph 11 above) entails the processing of personal data by automated means and as a result it is subject to the provisions and data protection principles of Part 3 of the DPA 2018.[32] Moreover, AFR technology involves "*sensitive processing*" of personal data pursuant to section 35(8)(b) of the DPA 2018 as it involves "*the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual*". AFR technology data processing is therefore subject to the further, more stringent requirements for sensitive processing set out in section 35(5) of the DPA 2018.

47. SWP's ongoing use of AFR technology breaches the first and third data protection principles as set out in Part 3 of the DPA 2018.[33]

48. The first principle states that the processing of personal data must be lawful and fair.[34] In order to be lawful, the processing must be "*based in 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.*"[35] Furthermore, due to AFR processing being categorised as sensitive processing by the DPA 2018, it is only permitted where "*the processing is strictly necessary for the law enforcement purpose… and at the time when the processing is carried out, the controller has an appropriate policy document in place.*"[36]

49. For the reasons explained at paragraphs 13 to 14 above, it is clear that the data processing through AFR technology is not adequately "*based in law*" or adequately regulated by any statute or regulatory legal framework. In addition, it cannot be said that the indiscriminate scanning and analysis of the faces of all members of the public within range of the AFR technology is "*strictly necessary for the law enforcement purpose*" of the technology. ICO guidance notes that "*[s]trictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means*".[37] SWP's use of the technology as part of its day-to-day policing strategy, for example on shoppers on Cardiff's Queen Street, is certainly not a pressing social need and the same law enforcement aims could be (and hitherto have been) achieved through far less intrusive means such as normal CCTV or police presence. For these reasons, the ongoing use of AFR technology fails to meet the

---

32 s.29(1)(a) DPA 2018.
33 ss.35-37 DPA 2018.
34 s.35(1) DPA 2018.
35 s.35(2) DPA 2018.
36 ss.35(3) and (5) DPA 2018.
37 'Guide to Law Enforcement Processing (Part 3 of the Bill)', 5 April 2018, available here: https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-bill/conditions-for-sensitive-processing/.

requirements of the first data protection principle.

50. The third data protection principle is that "*personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.*"[38] By scanning the faces of potentially thousands of innocent passers-by, the vast majority of the personal data processed by AFR technology is irrelevant to its law enforcement aims and is of no legitimate use to SWP. Moreover, the quantity of personal data that is processed by AFR technology, nearly all of which concerns members of the public engaging in lawful activities, is excessive and unnecessary. The ongoing use of AFR technology is therefore not compliant with the third data protection principle.

Breach of the DPA 1998 through use of AFR technology against my client

51. By deploying AFR technology against my client on 21 December 2017 and 27 March 2018 (as described above), SWP breached its obligations under section 4 of the DPA 1998 (in force until 25 May 2018) taken with the first data protection principle, which provided that: "*Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless…at least one of the conditions in Schedule 2 is met.*"[39]

52. SWP's processing of my client's personal data was not fair or lawful for the reasons set out above and it did not satisfy any of the conditions in Schedule 2 to the DPA 1998. For the avoidance of any doubt, SWP cannot rely on section 29 of the DPA 1998 for the reasons set out at paragraph 33 above.

53. My client deeply values his privacy and has been caused considerable distress by the knowledge that his biometric personal data were captured and stored by SWP. In respect of the processing of my client's personal data at and in connection with the Cardiff Arms Fair, his distress was compounded by the highly intimidating nature of SWP's use of AFR technology at that event. Pursuant to section 13 of the DPA 1998 (taken with *Vidal-Hall v Google* [2016] QB 1003), he seeks compensation from SWP for the distress that he has suffered as a result of SWP's breach of the DPA 1998.

Remedy sought

54. SWP is asked to confirm that it accepts that:

    a) its ongoing use of and recourse to AFR technology is unlawful in that it breaches Articles 8, 10, 11 and 14 of the ECHR, the PSED, and the first and third data protection principles in Part 3 of the DPA 2018; and

    b) its use of AFR technology against my client in Cardiff on 21 December 2017 and 27 March 2018 violated his rights under Articles 8, 10 and 11 of the ECHR and the DPA 1998.

55. SWP is also requested to:

    a) cease using AFR technology with immediate effect; and

---

38 s.37 DPA 2018.
39 Sch. 1, para. 1 DPA 1998.

b) make a reasonable offer of compensation for breaching my client's ECHR and DPA 1998 rights.

The details of any documents that are considered relevant and necessary

56. If SWP is not prepared to agree the remedy set out above, my client seeks disclosure of the following:

a) Any and all documents showing SWP's rationale for using AFR technology;

b) Confirmation of when the draft Privacy Impact Assessment was first prepared and provision of any earlier iterations of it;

c) Copies of all codes of practice, policy statements, manuals, memoranda, presentations, training materials or other records governing the use of AFR technology by SWP, including any such materials received from the Home Office;

d) Confirmation of whether SWP sought validation of the AFR system from the Surveillance Camera Commissioner, consistent with the COP 2013, paragraph 3.2.3, footnote 4. If so, disclosure of the correspondence and validation;

e) Copies of all policies, guidance notes, briefings or other similar material for SWP officers on the use of AFR technology;

f) Copies of all planning documents, logs and records relating to SWP's use of AFR technology since it began using it;

g) Copies of all consultations with the Information Commissioner, Biometrics Commissioner, Surveillance Camera Commissioner, Home Office Biometrics Programme, College of Policing, and the National Law Enforcement Database Programme about the use of AFR technology by SWP;

h) Operational and technical standards for AFR Locate;

i) A summary of the dataset used to train AFR Locate, including by reference to gender and ethnicity, both original and any updates to it;

j) Disclosure of all available demographic data pertaining to the false positive matches using AFR technology, in particular gender and ethnicity;

k) Confirmation of the sources of the control data and/or a summary of the type of known offenders that are being included in that data (by offence category);

l) Copies of all reviews of AFR technology, pursuant to guiding principle 2 from the COP 2013;

m) Any equality impact assessment that has been undertaken in respect of the use of AFR technology;

n) Confirmation of whether the AFR technology deployed by SWP also has an audio recording function. If so, we ask that you confirm whether such function was in use at the Cardiff Arms Fair in March 2018;

o) Confirmation of whether or not you have undertaken a data protection impact assessment concerning the use of AFR technology pursuant to the requirements of Article 35 of the GDPR. If so, please provide us with a copy of the same; and

p) Confirmation of whether or not you are processing any personal data of which my client is the subject; and

q) Any other relevant records in the possession of SWP.

Proposed reply date

57. We would be very grateful for your response within 14 days, i.e. **by no later than 25 June 2018**. This timeline is proposed on the basis that the intended claim is a challenge to an ongoing decision, meaning that there is no longstop date while SWP continues to use AFR technology as described above. Nonetheless, it is our client's intention to issue his claim in early July, following receipt of your response and assuming that liability is denied.

58. For the avoidance of doubt, because my client's claim concerns the ongoing use of AFR technology in the SWP policing area, he does not consider that the limitation period begins to run from the date he believes he was last personally captured (27 March 2018). If you do not agree with this assessment, please let me know by return with your reasons by **no later than Friday 15 June 2018**, so that we can consider whether time ought to be abridged for your response and proceedings issued within 3 months of the date my client believes he was last personally captured.

Address for reply and service of court documents

59. As noted above I am instructed to represent Mr Bridges. His address for service is:

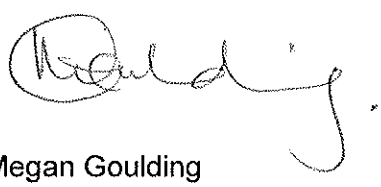
Megan Goulding
Liberty House
26-30 Strutton Ground
London
SW1P 2HR

Tel: 020 7378 3651

Email: MeganG@libertyhumanrights.org.uk

60. Please note that, unless agreed otherwise, I do not accept service by email. I am, however, happy to receive your response to this letter by email.

Yours sincerely



Megan Goulding
Solicitor
Liberty