Leigh Day

Direct Dial: 020 7650 1240
Email: adews@leighday.co.uk
Your Ref:
Our Ref: ADS/REC/00181394/1
Date: 13 June 2018

The Secretary of State for the Home Department
Litigation Operations Allocation Hub
Status Park 2
4 Nobel Drive
Harlington
Hayes
Middlesex
UB3 5EY

By post and email: public.enquiries@homeoffice.gsi.gov.uk

Dear Home Secretary,

Letter before claim: UK police use of Automated Facial Recognition ('AFR') technology

We are instructed on behalf of Jenny, Baroness Jones of Moulsecoomb and Big Brother Watch.

Our clients are concerned about the use of automated facial recognition ("AFR") technology by the police. We are writing to ask you to withdraw Home Office support for AFR technology. If it is your position that AFR is a strictly necessary and proportionate tool for police to use, we ask that you demonstrate that the interference with articles 8, 10 and 11 of the European Convention of Human Rights (ECHR) is necessary and proportionate to a legitimate aim and that you take such steps as are available to you to bring about a regulatory framework governing the use of AFR technology that satisfies the ECHR requirements in the terms described below.

If you do not confirm that you will do so, our clients may make a claim for judicial review, seeking a declaration that the use of AFR technology, and the absence of a sufficient legal framework for it, is unlawful. Baroness Jones is a victim within the meaning of s.7 of the Human Rights Act 1998, in part because she runs the risk of being affected by, and is required to modify her conduct because of, the matters challenged.

Please treat this letter as a letter before claim for judicial review. We would be grateful if you could reply within 14 days – i.e. by **close of business on 28 June 2018.**

Background

Big Brother Watch recently published a report named '*Face Off: The lawless growth of facial recognition in UK policing*'.[1] Additional factual background is contained in that report, and we would be grateful if you could refer to that if you would like further detail.

It appears that one way AFR technology is currently being used is that a 'watch list' of images is compared by the facial recognition system against the facial image captured live by a CCTV camera. The AFR technology converts the facial image into a unique code that functions as a biometric identifier. It then decides whether the biometric identifier created from the CCTV facial image matches that of the 'watch list' facial image. If so, the CCTV facial image and code are stored by the police, together with associated data such as the location where and the time when the image was taken.

Individuals who have been scanned by AFR technology are often unlikely to know that is the case. The subject does not have a choice whether they are scanned by AFR or whether their image and biometric data is retained, and cannot challenge the retention of that information, especially if they were not aware that they were subject to AFR.

As well as data being retained by the police, a 'match' may lead to other detriments to an innocent subject, such as disclosure of the data, being stopped by the police, being asked for proof of identity, and perhaps being removed from the location or event where the AFR technology is being used.[2]

We also attach a letter written to the Commissioner of Police for the Metropolis. The letter contains further information about the use of the technology by that force.

We understand that the Home Office provides support for the use of AFR, in particular considerable financial support for the development and introduction of the technology.

The effects of AFR on my clients

Baroness Jones has substantial concerns about police use of AFR, the significant negative effect it would have on their work, and the detriment it would cause to their daily activities.

---

[1] Big Brother Watch (2018) (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital.pdf)

[2] Metropolitan Police News, *Notting Hill Carnival 2016*, 26 August 2016 (http://news.met.police.uk/news/notting-hill-carnival-2016-181523)

Baroness Jones is concerned that police use of AFR could identify and thus interfere with confidential meetings with whistleblowers and campaigners with whom she meets regularly as part of her Parliamentary duties as a Member of the House of Lords. She is concerned that AFR may record, monitor or otherwise affect such meetings, as some of these individuals may be on the 'watch-lists' in relation to their campaigning work. She is concerned, for example, that police use of AFR could interfere with her confidential meetings with non-state core participants in the current Undercover Policing inquiry. She is also concerned that she will have to modify her conduct because she would be have to avoid meeting certain individuals in an area where AFR would or might be used.

Baroness Jones is concerned that police use of AFR may identify patterns of interactions between herself and her contacts to the police, which may include the actions or whereabouts of her contacts and/or identify them as campaigners or whistleblowers. She is also concerned that police use of AFR could identify an individual's political affiliations or political views, via association with her. This would significantly affect her Parliamentary work and could require her to take special precautions when meeting with certain individuals, or may force her to avoid meeting with them altogether, in order to protect them.

Baroness Jones has particular concerns about the sources of the images used by police to construct watchlists at AFR deployments, including uncertainty as to whether it is solely custody images that are used or images sourced from police surveillance teams at protests, the internet or social media, or other sources. Baroness Jones understands a photograph of her has been on a police database as she was listed on the Metropolitan Police's 'Domestic Extremism' database.

Baroness Jones has stated that if she were aware that police intended to use AFR at a particular event or in a particular area, it would cause her to avoid that event or area in order to protect her privacy and avoid unwarranted state intrusion. As a result, that could have a significantly detrimental effect on her work as a Member of the House of Lords and a Parliamentarian who regularly attends public events and demonstrations and gives talks at such events and demonstrations.

Overall, Baroness Jones believes that police use of AFR would significantly affect her Parliamentary activities and her ability to carry out her democratic functions as a Member of the House of Lords.

The national regulatory framework for AFR

There is no legislation regulating the use of AFR. Nor is there any other national instrument which contains any significant regulation.

The Surveillance Camera Code of Practice briefly mentions facial recognition technology: in particular see Principle 2 and § 4.12.1. However, there has been uncertainty as to whether the oversight of facial recognition technology comes within the ambit of the Surveillance Camera Commissioner (SCC) at all. The SCC, in 2016, stated:-

> "Clarity regarding regulatory responsibility is an emerging issue, **for example in automatic facial recognition use by police – which regulator has responsibility** – the Biometric Commissioner, the Information Commissioner or Surveillance Camera Commissioner." (emphasis added).[3]

The SCC returned to this theme and the uncertainty in this area in his most recent annual report, published in January 2018:

> "I engage regularly with Biometrics Commissioner particularly in relation to the issue of **automatic facial recognition technology**. At the time of writing I await publication of the Home Office Biometric Strategy which will, I hope, **provide much needed clarity over respective roles and responsibilities in this area**" (emphasis added).[4]

The SCC also said that "Currently there are gaps and overlaps in regulatory oversight of some of these issues; which regulator is responsible for oversight of use of AFR?"[5]

Baroness Williams, Minister of State for Countering Extremism, recently wrote a letter to Norman Lamb MP (Chair of the Science and Technology Committee) which stated her intention to provide some oversight of AFR as follows:

> "We will create a Board (to oversee facial recognition technology) including the three relevant regulators (the Biometrics Commissioner, Surveillance Camera Commissioner and Information Commissioner) and police representatives. This will (…) provide greater assurance that policing is complying with guidance".[6]

However, it is unclear what guidance this refers to, as there remains no legislation or regulation providing a basis for or policy for police use of AFR.

---

[3] Surveillance Camera Commissioner, *Review of the impact and operation of the Surveillance Camera Code of Practice,* February 2016, p.15

[4] Surveillance Camera Commissioner, *Annual Report 2016/17*, January 2018, pg. 20 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/672286/CCS207_CCS0118716124-1_Annex_A_-_AR_2017-_web.pdf

[5] *Ibid,* pg. 41

[6] Baroness Williams of Trafford, in a letter to The Rt. Hon Norman Lamb MP, 28 March 2018: https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

There is an obvious need for legislation, if AFR is deemed a necessary and proportionate technology for police to use. The Commissioner for the Retention and Use of Biometric Material (the "Biometrics Commissioner") explained this:

> "The use of facial images, especially in public places, is very intrusive of individual freedom, especially because images can be captured without the subject being aware. The public benefit of the use of such an intrusive technology must outweigh the interference in individual privacy. Such a difficult balance between public benefit and individual privacy should not be decided by the police but is best decided by Parliament through informed debate and legislation. As is currently the case for DNA and fingerprints the legislation should include independent oversight to reassure the public that their privacy is being properly protected."[7]

The Information Commissioner has also commented on the lack of a regulatory and governance framework for police use of AFR:

> "I have been deeply concerned about the absence of national level co-ordination in assessing the privacy risks and a comprehensive governance framework to oversee FRT [Facial Recognition Technology] deployment."[8]

Legal background

The use of AFR violates articles 8, 10 and 11 of the European Convention on Human Rights, and is unlawful due to section 6 of the Human Rights Act 1998. I focus here on article 8. The reasons why the use of AFR technology breaches articles 10 and 11 are analogous.

(i) Interference

The use of AFR constitutes a significant interference with the article 8 rights of the person whose image is processed and retained. AFR may be used to identify, monitor or track an individual, and this surveillance normally operates covertly. The data stored when there is a match, including a person's image, the related biometric identifying data, the person's location, the time they were there, and associated data, is sensitive. It is not clear how long police forces

---

[7] Biometrics Commissioner, *Metropolitan Police's use of Facial Recognition Technology at the Notting Hill Carnival*, 23 August 2017 (https://www.gov.uk/government/news/metropolitan-polices-use-of-facial-recognition-technology-at-the-notting-hill-carnival-2017)

[8] Information Commissioner, *Blog: facial recognition technology* (https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology/)

currently and have historically retained the images, biometric data, and associated information. Until recently, South Wales Police was retaining even false positive images for 12 months. If other action is taken against the subject as a result of a 'match', such as being stopped by police, monitored, or their AFR data used or disclosed to and used by other bodies, there is likely to be a more substantial interference. It is clear that the application of AFR is a matter of serious concern for at least part of the public. It is relevant that there is a very high risk of a false positive match.

(ii) In accordance with the law

Any interference with article 8 must be "in accordance with the law". In general, this means the interference must have a basis in domestic law which is accessible and foreseeable, and there must be adequate and effective guarantees against abuse.[9]

The requirements of article 8 depend to some extent on the context. The present context calls for more onerous safeguards (for the reasons set out above).

In *Szabó and Vissy v Hungary*,[10] the ECtHR noted the "remarkable progress" in the scale and sophistication of surveillance technology in recent years, which have "reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread".[11] The court called for the "simultaneous development of legal safeguards securing respect for citizens' Convention rights". [12]

The ECtHR has developed "*minimum standards*" in order to ensure that the law provides sufficient guarantees against abuse, that should be set out in "*statute law*" as "*clear, detailed rules*", rather than internal or other forms of law.[13] In *M.M. v United Kingdom*, the European Court of Human Rights ('ECtHR') recognised that in *Khan*, Article 8 had been violated "because there existed no statutory system to regulate the use [of covert listening devices] and the guidelines applicable at the relevant time were neither legally binding nor directly publicly accessible".

The law must also be formulated with sufficient precision to enable the individual to regulate his or her conduct: *S v. United Kingdom* [2009] 48 EHRR 50, §95. It must indicate with

---

[9] *Klass v Germany* (1978), § 43-44 and 50; *Malone v UK* (1984), § 66, 68 and 79; *Weber v Germany* (2006), § 84; *Gillan and Quinton v UK* (2010), § 76-77.

[10] (2016) ECHR App. No. 37138/14

[11] § 68

[12] *Ibid*

[13] *Weber*, § 92 and 95.

sufficient clarity the scope of any discretion conferred on the competent authorities and the manner of its exercise. There must be:

> "clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness": *S v United Kingdom* [2009] 48 EHRR 1169, §99; *M.M. v. United Kingdom* (24029/07) 13 Nov 2012 §195.

In addition, there must be safeguards which have the effect of enabling the proportionality of an interference to be adequately examined: *R (T) v. Chief Constable of Greater Manchester* [2015] AC 49, §114. Rules which lead to a retention of data for a fixed period, or the blanket disclosure of material, where that retention or use may not be justified, have been held to breach article 8. For example, reliance on the MOPI policy was said to be unlawful in relation to the retention of custody photographs in *R (C) v Metropolitan Police Commissioner* [2012] 1 WLR 3007.

Both the CJEU[14] and the ECtHR[15] have identified a requirement for *ex post facto* notification, in the context of covert surveillance. Since AFR matches and simultaneous biometric photography are ordinarily conducted in an essentially covert way, any regulatory regime ought to provide for notification where practicable.

Public law normally requires that a policy applied by a public body is published: *R (Lumba) v Secretary of State* [2012] 1 AC 245, at §35 and 38. Similarly, article 8 requires the law to be "accessible to the person concerned and foreseeable as to its effects".[16]

In *Shimovolos v Russia*[17] the ECtHR found a violation of Article 8 where police had created a database on the basis of a ministerial order, but the public could not know what type of information was included and for how long, how it was stored and used, or who had control over it. This is similarly the case with information collected and retained as the result of the police use of AFR: where the system creates a false positive, that facial biometric data, and the image of the innocent person who has been scanned and subsequently mismatched, is then retained by the police for an amount of time which is unclear and inconsistent.

---

[14] Joined Cases C-203/15 *Tele2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970) ("Watson"), § 121.

[15] § 86

[16] *Zakharov v Russia* (2015), App. No. 47143/06, 4 December 2015, § 228; *Catt* §11; and *Shimovolos v. Russia* (30194/09) 21 June 2011, §69

[17] (2011) ECHR App no. 30194/09

(iii) Necessary in a democratic society

Even if a measure has been taken in pursuit of one of the legitimate interests in Article 8(2), the measure must be necessary. The ECtHR has held that the concept of "necessity" implies two things: (i) that any interference corresponds to a pressing social need; and (ii) that it is proportionate to the legitimate aim pursued.

The basic framework for deciding whether an interference is necessary is to ask first whether the objective behind the interference was sufficiently important to justify the interference with the rights under article 8; second whether the measures were rationally connected to the objective; third whether they went no further than was necessary to accomplish it; and fourth, standing back, whether they struck a fair balance between the article 8 rights of the applicant and the interests of the community: see, e.g. *R (T) v. Chief Constable of Greater Manchester* [2015] AC 49 at §39. This is often a fact specific question, based on common sense considerations. An example of the retention of an image being held not to be 'necessary in a democratic society' is *R (Wood) v. Commissioner of Police of the Metropolis* [2010] 1 WLR 123.

Following *S v United Kingdom*[18], the Court of Appeal in *R (Wood) v Metropolitan Police Commissioner*[19] made clear that an interference with Article 8 could be justified if it was proportionate to the interference.[20] Although Wood's photo was not used for spotter cards, its retention was nevertheless disproportionate. Furthermore, the court stated that:

> "[T]he justification must be the more compelling where the interference with a person's rights is, as in the present case, in pursuit of the protection of the community from the risk of public disorder or low level crime"[21]

In relation to the third element of the framework set out by the ECtHR, that the measure taken to achieve the objective went no further than was necessary to achieve it, the ECtHR has considered whether the aim pursued could have been achieved by a less intrusive method: see e.g *Bărbulescu v. Romania* (application no. 61496/08) §121. The Information Commissioner has commented on this element, stating that: "For the use of FRT to be legal, the police forces must have clear evidence to demonstrate that the use of FRT in public spaces is effective in resolving the problem that it aims to address and that no less intrusive technology or methods are available to address that problem."[22]

---

[18] (2008) ECHR 178

[19] [2009] EWCA Civ 414

[20] *Ibid*, § 81

[21] [2009] EWCA Civ 414, § 86

[22] Information Commissioner, *Blog: facial recognition technology* (https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology/)

EU Law contains similar requirements in this context to the ECHR. The CJEU considered the retention of location data, inter alia, in *Tele2 Sverige v Post- och Telestyrelsen and Secretary of State for the Home Department v Tom Watson.*[23] The court ruled that even an objective of general interest, such as "the fight against serious crime", however fundamental that fight may be, "cannot in itself, justify that national legislation providing for the general and indiscriminate retention of all (…) location data should be considered to be necessary for the purposes of that fight."[24] The court also held that EU law must be interpreted as "precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all… location data".[25]

Reasons why the defendant's conduct is unlawful

The use of AFR technology interferes with the ECHR. The interference is not "in accordance with the law", for the following reasons.

There is no legislative framework governing the use of AFR which satisfies the minimum standards set out by the ECtHR. The PoFA provides no statutory framework within which AFR is used. All that is present is a requirement for a statutory code of practice in relation to the use of surveillance camera systems. However, PoFA specifically states that not all uses of surveillance cameras need to be included in the code, and the reason for that is because of the difficulty of providing a code for emerging technologies (such as AFR).

The PoFA provides for a Surveillance Camera Commissioner and for a Biometrics Commissioner, but both Commissioners have highlighted confusion and uncertainty about which Commissioner is responsible for AFR, while highlighting the need for a proper statutory framework for its use.[26] The Surveillance Camera Code of Practice, published in 2013 prior to the advent of AFR in UK policing, states only that AFR: "needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated."[27]

Current legislation and policy leaves open many questions as to the scope and application of AFR technology, and contains none of the requisite minimum safeguards. For example, it does not define:

---

[23] Joined Cases C-203/15 *Tele2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970) (21 December 2016)

[24] *Ibid,* § 103

[25] *Ibid*, § 112

[26] Surveillance Camera Commissioner, *Annual Report 2016/17*, January 2018, pg. 41 and pg. 20;
Surveillance Camera Commissioner, *Review of the impact and operation of the Surveillance Camera Code of Practice,* February 2016, p.15;
Biometrics Commissioner, *Metropolitan Police's use of Facial Recognition Technology at the Notting Hill Carnival*, 23 August 2017

[27] Home Office, *Surveillance Camera Code of Practice*, June 2013, §. 3.2.3

1. Which categories of individuals, and which databases, are used for the watch list images.
2. The criteria which are used to decide whether a person will be included on the watch list.
3. Who decides whether the criteria are met
4. What steps will be taken to ensure the watch list images are accurate.
5. When there is a match, what information is stored
6. How long is that information stored for, including in respect of a false positive
7. Where the information is stored.
8. Who may have access to it
9. In what circumstances may those people or bodies have access to it
10. For what purposes the information may be used.
11. What action may be taken as a result of a match
12. The circumstances in which that action may be taken.
13. Who decides whether to take that action

In effect, there are very few if any safeguards against abuse for this particular technology and its unique implications for individuals' rights. There are no restrictions on the application of AFR, and there are no safeguards in national law to prevent an individual from being subjected to arbitrary treatment.

The situation is exacerbated by the unsatisfactory legal and policy position in relation to custody images. It is understood that there are hundreds of thousands of people whose images are being retained unlawfully, despite the decision in *R (C) v Metropolitan Police Commissioner* [2012] 1 WLR 3007. To the extent that AFR technology allows the police to compare images against this database, including by creating 'watch lists' of individuals using images from this database, another level of unlawfulness is introduced to the system.

Thus, the lack of a statutory regime, the lack of codes of practice, uncertainty as to when and where AFR can be used, the absence of public information and rights of review, and the use of custody images unlawfully held, are all factors which indicate that the use of AFR, and the use and retention of data as a result of this, are not in accordance with the law for the purposes of article 8(2).

The interference is also not "necessary in a democratic society". This issue overlaps with the question of whether the interference is in accordance with the law. Thus, it is disproportionate to interfere with rights to respect to private life using procedures and technology which do not have a sufficient legal basis and policy framework, and where the safeguards against abuse are non-existent. The indiscriminate use of AFR is not proportionate to the legitimate aims of the prevention and detection of crime and the protection of others. This issue is only exacerbated where such a significant number of matches are false. It is for the government to demonstrate

that the interference with articles 8, 10 and 11 is necessary and proportionate to a legitimate aim, and you have not done so.

The use of AFR is contrary to EU Law and public law for reasons which overlap with those set out above in respect of the ECHR. Since the use of AFR is unlawful, the financial support the Home Office provides for it is also unlawful.

Action the defendant is requested to take

Please confirm that you will withdraw Home Office support for AFR technology. If it is your position that AFR is a strictly necessary and tool for police to use, I ask that you demonstrate that the interference with articles 8, 10 and 11 of the European Convention of Human Rights (ECHR) is necessary and proportionate to a legitimate aim, in which case we ask that you take such steps as are available to you to bring about a regulatory framework governing the use of AFR technology that satisfies ECHR requirements.

The regulatory framework should be national legislation that prohibits the use of AFR unless and insofar as the government demonstrates that it is strictly necessary and proportionate to a legitimate aim. Alternatively, if AFR may be used, the regulatory framework must satisfy the requirements of the law set out above, for example by being 'in accordance with the law' within the meaning of article 8 ECHR. If you agree to do so, please detail exactly what steps you will take, when you will take them, and what the contents of the framework will be.

If you decline to do so, please:

1. Explain why.
2. Disclose to us any other material you may rely on in defending a judicial review challenge to the use of AFR.
3. Explain whether you agree with or dispute the contents of this letter.
4. If you dispute any of this, please identify what you dispute and why.
5. If you are responsible for any policy governing the use of AFR please identify it and disclose a copy to me.

Please reply by email and post by close of business on 28 June 2018, including copies of any relevant documents, to the below address:

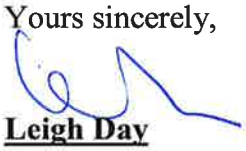
Leigh Day Solicitors, Priory House, 25 St John's Lane, London, EC1M 4LB
rcurling@leighday.co.uk and adews@leighday.co.uk

If you do not respond in the terms requested above and in the time specified, we may issue judicial review proceedings against you without further notice, and will necessarily be put to

the cost of doing so. If you subsequently comply with our client's request, or if we obtain a court order granting the same, then we will consider you liable for our costs in full.

Please confirm receipt of this letter.

Yours sincerely,



Leigh Day

Cc: Government Legal Department, Public Law Team