Birkbeck
UNIVERSITY OF LONDON

BIROn - Birkbeck Institutional Research Online

Keenan, Bernard (2021) Automatic facial recognition and the intensification of police surveillance. Modern Law Review 84 (4), pp. 886-897. ISSN 1468-2230.

Downloaded from: https://eprints.bbk.ac.uk/id/eprint/43209/

Usage Guidelines:
Please refer to usage guidelines at https://eprints.bbk.ac.uk/policies.html or alternatively contact lib-eprints@bbk.ac.uk.

Case Comment: *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058

Automatic facial recognition and the intensification of police surveillance

Word count: 4504 **including footnotes:** 4920

Statement: This material is not under consideration elsewhere and has not been published nor is it pending publication elsewhere.

Keywords: Facial recognition, surveillance, privacy, Article 8, policing, discrimination

Abstract: In *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 the Court of Appeal held the deployment of live automated facial recognition technology (AFR) by the South Wales Police Force (SWP) unlawful on three grounds.[1] It violated the right to respect for private life under Article 8 of the European Convention on Human Rights (ECHR) because it lacked a suitable basis in law; the Data Protection Impact Assessment carried out under section 64 of the Data Protection Act 2018 was deficient for failing to assess the risks to the rights and freedoms of individuals processed by the system; and SWP failed to fulfil the Public Service Equality Duty (PSED) imposed by section 149 of the Equality Act 2010 by failing to assess whether or not the software used in the AFR system was biased in relation to sex and race.

* Unless otherwise stated, all URLs were last accessed 22 October 2020.

[1] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

This is a significant case. It marks the first time the courts have considered the legality of AFR deployed in the service of policing. It sets important parameters for its use in the future. This case commentary sets out the facts and explains the Court of Appeal's reasons for overturning the initial decision of the Divisional Court.[2] It then discusses the implications of the judgment for the use of AFR technology by police and advances criticism of the Court's approach.

Facts

The appellant is a civil liberties campaigner living in Cardiff. His case was supported by Liberty, the civil liberties organisation. The respondent is the Chief Constable of South Wales Police (*Heddlu De Cymru*). The Secretary of State for the Home Department, responsible for nationwide policing and for the development of technology like AFR, is an Interested Party, while the Information Commissioner and the Surveillance Camera Commissioner are intervenors.

SWP is the leading police force in trials of AFR in the UK and has been using the technology since mid-2017, beginning with that year's Champions League final at the Millennium Stadium in Cardiff. The trial system is called 'AFR Locate'. The facial recognition software used in AFR Locate is called 'NeoFace Watch'. It is proprietary software licenced from a company now called North Gate Public Services (UK) Ltd

[2] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) [2020] 1 WLR 672, [2020] 1 All ER 864.

(formerly NEC).[3] The software is also used in a system called 'AFR Identify' to compare images of unknown suspects and persons of interest against images stored in the SWP custody database (around 500,000 faces).[4] The latter system was not challenged in the case.

AFR Locate is deployed via CCTV cameras mounted on police vehicles or on poles to carry out live surveillance in crowded areas. It was used around 50 times between May 2017 and April 2019. In that period an estimated 500,000 faces were scanned. SWP aimed in each deployment to scan as many individual faces as possible. The vast majority were of no interest to the police.

The basic function of AFR Locate is explained in the judgment. First, a database of existing images – called the 'watchlist' – is compiled.

> The watchlist is created from images held on databases maintained by SWP as part of its ordinary policing activities, primarily from a database of custody photographs held on SWP's Niche Record Management System. The images selected for inclusion on a watchlist will depend on the purpose of each specific deployment. The watchlists used in the deployments in issue in this case have included (1) persons wanted on warrants, (2) individuals who are unlawfully at large (having escaped from lawful custody), (3) persons suspected of having committed crimes, (4) persons who may be in need of protection (e.g. missing

[3] n 2 above, at [26].
[4] ibid at [27].

> persons), (5) individuals whose presence at a particular event causes particular concern, (6) persons simply of possible interest to SWP for intelligence purposes and (7) vulnerable persons. To date, the watchlists used by SWP have comprised between 400-800 people. The maximum capacity for a watchlist is 2,000 images but, as we understand it, this is because of the limits of the technology used rather than any limitation of principle.[5]

Images selected for the watchlist on each deployment are processed in order to map and encode the biometric 'facial features' of the faces on the watchlist. Once deployed, the camera system generates a live visual feed, which is analysed in near-real time by the software. Individual faces are automatically detected and isolated as people pass into the field of observation. The software selects unique features from each facial image and encodes them as a biometric template unique to each individual. It compares the biometric templates generated from the crowd against the biometric templates generated from the watchlist. The comparison works by generating a 'similarity score' between each detected face and each face on the watchlist. The higher the score, the more likely that there is a positive match between a person in the camera feed and a person on the watchlist. The operator of the system must specify a threshold value for similarity scores above which the software will alert the operator of a potential match. The lower the threshold, the greater the 'false alarm rate', as less likely matches are flagged up for human attention. The higher the threshold, the more likely it becomes that a true match will be missed by the operator and a potential target

[5] n 1 above, at [13].

escapes detection.[6] Where a match was flagged up by the system the operator reviews the images to confirm the match and, if positive, decides on what action to take.[7]

During the trial, all biometric templates produced from the live stream were immediately deleted. All data derived from faces that did not match against the watchlist were immediately erased. Images of matched faces were stored for 24 hours but the biometric template was not. The raw CCTV feed was recorded and stored for 31 days, as per the standard CCTV retention period. Watchlist images and biometric data were erased from the system within 24 hours of deployment.[8]

AFR Locate was not used covertly. SWP advertised each deployment on social media, placed large 'Fair Processing Notices' on the vehicles and in a 100-meter radius from the area under surveillance, and handed out postcard-sized information leaflets to passers-by and to everyone stopped as a result of the AFR Locate system. Nonetheless, many people scanned by the system would have been unaware of its presence.[9]

Judicial review

Mr Bridges claimed his face was detected and processed by AFR Locate on two occasions, first in December 2017 in Cardiff city centre and again in March 2018 at a

[6] ibid at [9].
[7] ibid at [15].
[8] ibid at [17]-[18].
[9] ibid at [19]-[20].

protest.[10] Judicial review was sought on the grounds that SWP's deployment of AFR Locate on these occasions was not compatible with the right to respect for private life under Article 8 of the ECHR, that it breached aspects of the Data Protection Act (DPA) 1998 and the DPA 2018, and that SWP had failed to meet the PSED imposed by section 149 of the Equality Act 2010.[11] SWP could not confirm whether or not Bridges had indeed been scanned, but accepted that he was a victim for the purposes of section 7 of the Human Rights Act 1998. Indeed, SWP and the Home Secretary consented to the application for judicial review.[12] Furthermore, the latest event Mr Bridges complained of preceded the commencement of the DPA 2018 (25th May 2018) by two months, however, all parties agreed to consider the law as it now stands.[13] This hypothecation of facts shows the utility of judicial review to the police and the Home Office, willingly putting their technological trial on trial before the law.

On 4th September 2019 the Divisional Court dismissed the claim on all grounds. The Divisional Court agreed that Article 8 was engaged in respect of anyone whose face is scanned by AFR Locate but held that the interference with privacy was both 'in accordance with the law' and proportionate for the purposes of Article 8(2). It was in accordance with the law because there was a sufficient legal framework in place, drawing together primary legislation, secondary legislation in the form of codes of practice issued under primary legislation, and SWP's local policies.[14] It was

[10] ibid at [25].
[11] ibid at [32]-[33].
[12] ibid at [34}.
[13] n 2 above, at [109].
[14] n 1 above, at [43].

proportionate, both in relation to any individual interference with Mr Bridges' rights on the dates in question and in general systemic terms,[15] for the following reasons:

> 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 neither occasion did it lead to a disproportionate interference with anybody's Article 8 rights […] the interference would be limited to the near instantaneous 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.[16]

With respect to the DPA 1998, the Divisional Court found that AFR Locate did process personal data but held that it did so lawfully and fairly in line with section 4(4) DPA 1998.[17] In respect of the DPA 2018, the Court agreed with the claimant that AFR Locate entails processing sensitive data for the purposes of section 35(8) as it uniquely identifies individuals, but found this processing lawful for three reasons. First,

[15] ibid at [44].
[16] n 2 above, at [101], cited in n 1 above, at [133].
[17] n 1 above, at [47].

because it is 'strictly necessary for the law enforcement purpose' as per section 35(5)(a), for the same reasons that the deployment of AFR Locate was found to be proportionate for the purposes of Article 8; second, in line with section 35(5)(b) the deployment complied with the necessary conditions for lawful sensitive processing specified in Schedule 2, again for the reasons given in the proportionality assessment, as well as SWP's common law duty to prevent and detect crime. Third, section 35(5)(c) requires SWP to have an appropriate Policy Document in place, compliant with the requirements of section 42. This particular issue was left open in anticipation of forthcoming guidance from the Information Commissioner.[18] The Court held that the Data Protection Impact Assessment (DPIA) undertaken by SWP in respect of the AFR Locate trial satisfied the requirements of section 64 DPA 2018.[19]

Finally, the Divisional Court rejected the claim that SWP had failed to discharge the PSED imposed by section 149 of the Equality Act 2010 when carrying out the relevant Equality Impact Assessment ahead of the trial by not considering whether or not AFR Locate could be indirectly discriminatory in its effect. The Court held that SWP did not have to consider the possibility because there was no evidence suggesting that NeoFace Watch software produces a higher rate of positive matches for female faces or for black and minority ethnic faces than for white or male faces.[20]

Appeal

[18] ibid at [50].
[19] ibid at [51].
[20] ibid at [52].

Permission to appeal was granted on all five submitted grounds:

1. That the Divisional Court erred in finding that the interference with the appellant's Article 8 rights was, and is, in accordance with the law.
2. That the Court made in an error of law in basing its proportionality assessment on the appellant's individual rights alone rather than also considering the cumulative weight of interference with the rights of all those persons whose biometrics were captured by the system during its deployment.
3. That the Court erred in its assessment of the DPIA under section 64 DPA 2018 by failing to factor in the engagement of Article 8, and the processing of the biometric personal data under the DPA, in respect of all who were processed by AFR Locate but not matched to watchlists.
4. That the Court made an error of law when it declined to reach a finding as to the compliance of SWP's November 2018 Policy Document with the requirements of section 42 DPA 2018, as the document is a condition precedent for lawful processing under section 35 DPA 2018.
5. That the Equality Impact Assessment carried out by SWP was obviously inadequate and failed to recognise the risk of indirect discrimination, that SWP's subsequent approach to the question of indirect discrimination is flawed, and that the Court erred in failing to appreciate that the PSED is an ongoing duty and not a single event.[21]

[21] ibid at [53].

In its judgment the Court of Appeal finds in favour of the appellant on the first, third and fifth grounds and rejects the second and fourth.

In respect of the first ground, the Court of Appeal adopts the 'relativist' approach proposed by Laws LJ in a partly dissenting judgment in *R (Wood) v Metropolitan Police Commissioner* when deciding on the quality of law required in order for the trial to be 'in accordance with the law'.[22] Put simply, this means that 'the more intrusive the act complained of, the more precise and specific must be the law said to justify it'.[23] This allows for an original assessment of the particular features of AFR Locate to be made by the Court of Appeal, informed by, but independent of, assessments made in relation to other surveillance technologies.

AFR Locate was compared by the Appellant to police retention of biometric fingerprint and DNA data from anyone arrested, regardless of whether they were charged or convicted. That was held unlawful by the European Court of Human Rights because it is unnecessary in a democratic society in the case of *S v United Kingdom*.[24] Once the issue of necessity was decided, the question of 'in accordance with the law' was not considered. Against this SWP drew an analogy with the case of *R (Catt) v Association of Chief Police Officers*,[25] in which the police's common law power to collect, retain, and use personal data concerning individuals who had attended

[22] *R (Wood) v Metropolitan Police Commissioner* [2010] WLR 123, [2009] 4 All ER 951 at [53].
[23] ibid.
[24] *S v United Kingdom* (2009) 48 EHRR 50.
[25] *R (Catt) v Association of Chief Police Officers* [2015] 2 All ER 727

public protests – the so-called 'extremism database' – was held to be in accordance with the law by Lord Sumption, giving judgment in the Supreme Court.[26]

For the Court of Appeal, AFR Locate lies somewhere between the two. The Court notes the following features:

> 86. First, AFR is a novel technology.
>
> 87. Secondly, it involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police.
>
> 88. Thirdly, it is acknowledged by all concerned that this is "sensitive" personal data, within the meaning of the DPA 2018. That Act in turn reflects EU legislation. This represents an institutional recognition of the sensitivity of the data concerned, a feature which is not present for example for ordinary photographs.
>
> 89. Fourthly, the data is processed in an automated way.[27]

On this basis the Court of Appeal finds two 'fundamental deficiencies' with the existing legal framework, which it refers to as the 'who question' and the 'where

[26] n 1 above, at [65], [79]-[80]. The Court of Appeal notes at [81] that the European Court of Human Rights disagreed with the proportionality assessment of the UK Supreme Court, finding that the surveillance of Mr Catt constituted a disproportionate violation of Article 8 in Catt v United Kingdom [2019] ECHR 76.
[27] n 1 above, at [86]-[89].

question': it does not make clear who may be placed on the watchlist, nor does it delimit where it can be lawfully deployed.[28] The Privacy Impact Assessment produced by SWP states that the watchlist could contain information pertaining to 'persons wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence is required'.[29] The first three of these categories the Court of Appeal finds to be 'objective', but the final category 'could cover anyone who is of interest to the police. In our judgement, that leaves too broad a discretion vested in the individual police officer to decide who should go onto the watchlist.'[30] The 'where question' is not addressed at all in existing law or guidance. In effect, 'the range is very broad and without apparent limits'.[31]

The Court also prescribes a third element: a requirement to delete all data pertaining to persons who are scanned but not matched by the system. In SWP's AFR Locate trial this was a technical process. It must become a legal requirement:

> We would hope that that feature of the current scheme would not simply be set out in a policy document by way of description but that it would be made clear that such automatic and almost instantaneous deletion is required for there to be an adequate legal framework for the use of AFR Locate.[32]

[28] ibid at [91], [104], [118]-[120].
[29] ibid at [123].
[30] ibid at [124].
[31] ibid at [130].
[32] ibid at [93].

The second ground concerning proportionality is addressed by the Court of Appeal notwithstanding the fact that the anterior finding of 'not in accordance with the law' was itself sufficient to dispose of the Article 8 issue. It raises an important question. The Appellant argued that the Divisional Court erred in law because it is necessary to consider the impact of AFR Locate not only on the appellant's individual rights but on the rights of all the members of the public captured by the system. In its judgment the Court of Appeal rejects this argument for two reasons. The first is procedural – the original claim for judicial review referred to the Appellant's rights alone.[33] More significantly, the Court goes on to hold that the impact on other members of the public:

> was as negligible as the impact on the Appellant's Article 8 rights. An impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement.[34]

On the third ground, the Court of Appeal agrees with the Appellant that the Data Protection Impact Assessment prepared by SWP is deficient for the purposes of section 64 of the DPA 2018. This inevitably follows from the finding that the deployment was 'not in accordance with the law' for the purposes of Article 8(2). As a consequence of the finding that the existing legal framework grants an impermissibly wide discretion to police officers in deciding who to place on the

[33] ibid at [142].
[34] ibid at [143].

watchlist and where the system can be deployed, it follows that the DPIA necessarily fails to properly assess the risks to the rights and freedoms of data subjects and to set out measures that could mitigate such risks.[35]

The fourth ground concerned an alleged error of law in the Divisional Court's decision not to make any finding on whether or not the content of the SWP Policy Document on AFR Locate was sufficiently detailed to comply with section 42 of the DPA 2018. The document was prepared in November 2018, but the Information Commissioner did not issue guidance on what a section 42 Policy Document ought to contain until November 2019. SWP updated the Policy Document accordingly. Given that the guidance from the Information Commissioner determined both the ability of SWP to issue a suitable Policy Document and the courts' ability to evaluate it, the approach of the Divisional Court is upheld.[36]

The final ground concerned the PSED under section 149 of the Equality Act 2010.[37] The Divisional Court held it was unnecessary for SWP to consider whether the technology was indirectly discriminatory because there was no positive evidence to suggest that the facial recognition software was biased along lines of race or sex. Citing the principles set out with authority in the case of *R (Bracking) v Secretary of State for Work and Pensions*,[38] the Court of Appeal emphasises that the PSED is a positive and continuing duty. It requires public authorities to proactively consider the potential

[35] ibid at [153].
[36] ibid at [160]-[161].
[37] ibid at [167].
[38] *R (Bracking) v Secretary of State for Work and Pensions* [2013] EWCA Civ 1345, [2014] Eq LR 60, at [26].

outcomes of a given measure, and to seek out relevant material regarding potential discriminatory effects by actively consulting with relevant groups where the material is not available. The Divisional Court's finding that the absence of positive evidence of bias leading to indirect discrimination means that the issue need not have been considered is to 'put the cart before the horse'.[39] While the Divisional Court had been content with SWP's submissions that it was reviewing the operation of the system against the requirements of section 149 on an ongoing basis as part of the technological trial, the Court of Appeal explicitly rejects this approach:

> The PSED does not differ according to whether something is a trial process or not. If anything, it could be said that, before or during the course of a trial, it is all the more important for a public authority to acquire relevant information in order to conform to the PSED and, in particular, to avoid indirect discrimination on racial or gender grounds.[40]

Instead, any police force planning to use an AFR system must first 'satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias'.[41]

Constraining mass surveillance

[39] n 1 above, at [182].
[40] ibid at [200].
[41] ibid at [201].

Automatic facial recognition is one of the most controversial products of the rapid rise in machine learning technologies. It is a potential tool of mass surveillance. As Foucault observed, governmental technologies are never simply oppressive. They are productive, and liberal governmentality is an exercise in balancing productive power against its counter-productive risks.[42] The productive potential of facial recognition technology is well known. It allows a face to function as an individual identifier in a wide array of uses. For example, it comes as standard on smartphones, which store biometric scans for use as cryptographic keys, allowing users to unlock devices or authorise transactions by glancing at the device. It is used widely on social media platforms, as when Facebook suggests who might be present in a photograph, simultaneously gaining data on users' interests and social lives.[43] In short, it grants smooth access to digital systems. Its potential risks as a surveillance tool are also well-known. For instance, following the Black Lives Matter protests that erupted across the United States in the summer of 2020, IBM announced it was abandoning the face recognition business, explicitly opposing its use for mass surveillance and racial profiling.[44]

This judgment places four important limits on the discretion of police in using facial recognition systems. First, the Court 'hopes' that the technical feature by which non-

[42] M. Foucault, Security, Territory, Population: Lectures at the Collège de France 1977-1978 (Basingstoke: Palgrave MacMillan, tr. 2007) 333-361.
[43] 'What is the face recognition setting on Facebook and how does it work?' (Facebook, 2020) available at https://www.facebook.com/help/122175507864081
[44] A. Hern, 'IBM quits facial-recognition market over police racial-profiling concerns' (9th June 2020) *The Guardian* https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns. Critics note that IBM was already relatively far behind its competitors in this market.

matched faces are deleted from the system becomes a normative rule. Automatic deletion is a key reason why the impact on Mr Bridges was deemed proportionate. AFR cannot be deployed to simply make a record of all the faces that passed through the targeted area. The implication of this is that for the Court, the processing of an unmatched face is a passive function of software; an intrusion on privacy so minimal as to be practically hypothetical. On this view, human rights are only materially affected if one is flagged up by the system as a potential match. The check by a human operator is regarded as a safeguard of privacy. No rights are materially impacted by the system until a police officer has confirmed the match is likely true and has decided on the appropriate course of action. It is argued below that this finding is constructed on a restrictive view of individual rights that inverts the logic of AFR and wilfully ignores considering its potentiality.

Second, and by implication of the previous point, the 'who question' governs all legally actionable decisions produced by the system. The law thus requires that there be an objective anterior legal justification for adding someone to the watchlist. Consequently, it would be unlawful to use AFR for prospective intelligence-gathering. Although the Court does not say so, it seems that the same requirement should apply by analogy to retrospective systems like AFR Identify, used by SWP to analyse footage of suspects drawn from existing CCTV networks, of which the UK has a vast number. The Court does not, perhaps understandably in this case, engage with the ongoing legal and political arguments as to whose biometric data is or should be retained in the Police National Database, how that data is handled and processed, and whether

or not it is deleted in accordance with the law. Inevitably the question of what necessary and proportionate police practices look like in a democratic society is a politically contested question, and one in which the UK consistently favours strong police powers.[45]

Third, the 'where' question means there must be anterior normative reason for deploying AFR in a given location. As with deletion of faces, this turns a technical limitation into a legal rule. It prevents police from unilaterally deploying live AFR systems broadly; for instance, across existing city-wide networks of CCTV cameras – again, an important point in the closely monitored public spaces of the UK. Yet precisely how a geographical area may be selected for deployment of AFR systems remains open and undefined.

Fourth, the PSED explicitly requires that software is checked for bias in advance of deployment. This should incentivise commercial developers of AFR technology to actually demonstrate that their algorithms produce consistently accurate results regardless of sex or race. This is a problem with AFR that has received much attention. A 2018 study by MIT and Stanford found an error rate of nought point eight per cent for light-skinned men and thirty-seven point four per cent for dark-skinned women.[46]

[45] Consider the recent ruling against the UK in *Gaughran v United Kingdom* (45245/15) [2020] 2 WLUK 607; Times, April 22, 2020 (ECHR); see also the findings in *Current and future uses of biometric data and technologies* HC 734 (2015) 3; and *Algorithms in the Criminal Justice System* (2019, The Law Society of England and Wales) 41.

[46] L. Hardesty. 'Study finds gender and skin-type bias in commercial artificial-intelligence systems' (11th February 2018) *MIT News* https://www.media.mit.edu/articles/study-finds-gender-and-skin-type-bias-in-commercial-artificial-intelligence-systems/

A December 2019 report from the US National Institute of Standards and Technology surveyed one hundred and eighty-nine commercial algorithms from ninety-nine different developers and found similar disparities.[47] The biases arise primarily from the manner in which neural networks that generate the algorithms are designed, and from the datasets on which they are 'trained'.[48] The Court heard evidence that the manufacturer of the NeoFace Watch software was unwilling to allow Mr Bridge's expert witness on facial recognition to inspect their software, citing commercial confidentiality. The Court makes clear that such concerns cannot excuse a public authority from its obligations under the Equality Act 2010.[49] Thus the need for public accountability trumps concerns over intellectual property. On this authority, all suppliers of algorithmic systems that perform governmental functions and which could potentially have a disproportionate impact on any line of differentiation covered by the Equality Act 2010 must open up the code to inspection. By the same token, government must ensure it has access to the expertise needed to objectively and effectively analyse any such programme for bias.

Liberty, the organisation which supported Mr Bridges in his case, is campaigning for a total ban on facial recognition.[50] That is a political position. As it stands, the judgment paves the way for the expansion of AFR within a defined legal framework.

---

[47] P. Grother, M. Ngan, K. Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (NISTIR 8280, December 2019) available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[48] ibid, 2.
[49] n 1 above, at [199].
[50] Liberty, 'Resist Facial Recognition' https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/.

While the principles enunciated by the Court of Appeal will ensure that the majority of the population will not be affected by AFR policing systems, it makes it acutely important to critically investigate how the 'objective' selection of watchlist targets and targeted areas intersects with, and intensifies, existing policing practices and databases. We should consider, for instance, who is affected when the watchlist is populated by protestors held on the 'extremism database', or with Home Office biometric data gathered from migrants and refugees. We should consider what happens when the 'where question' is answered by predictive algorithms purporting to predict where crime shall occur. Such algorithms work on data derived from past policing practices, reproducing and reifying existing biases.[51] If the majority are spared the dystopia of a generalised digital panopticon, it must not be at the expense of allowing minorities and marginalised communities to be subjected to intensified modes of pre-emptive police power.

Potentialities

There are two ways in which the judgment may hinder the future challenges to AFR which will inevitably arise. The first is, as mentioned, the refusal to consider that interference with privacy is more concerning when it is applied simultaneously to large groups than to individuals. As the Court puts it, 'An impact that has very little weight cannot become weightier simply because other people were also affected'.[52]

[51] H. Couchman, 'Policing by Machine: Predictive Policing and the Threat to Our Rights', Liberty, January 2019, available at https://www.libertyhumanrights.org.uk/issue/policing-by-machine/.
[52] n 1 above, at [143].

This may be true within the strictures of a positive system of individual rights, but it is obviously inadequate when confronting technologies that operate on the principle that individuals are simply elements within a larger population. It is the population, or segments thereof, that is placed under surveillance by AFR Locate. Targets emerge from the surveillance of the population on the basis of statistical analysis. When one enters a zone under AFR, whether one knows it or not, one becomes a potential target. That the processing has no direct impact does not lessen this potential impact. Being aware of such a potential in itself has a chilling effect, as long recognised by the law in relation to covert surveillance. The effect may indeed seem small on an individual but cumulatively it takes effect at the level of the population. This notion may be novel to the courts, but it is a point that has been persistently and persuasively made by scholars.[53] Privacy as an emergent social good should not be excluded from consideration in advance by cleaving to an individualistic model of rights. When considered at the level of the population rather than the individual, the question of whether or not the use of AFR is at all 'necessary in a democratic society' for the purposes of Article 8 may take on a different aspect.

The second, related, hindrance is the Court's refusal to adopt the dissenting judgment of Lord Kerr JSC in *Beghal v Director of Public Prosecutions*, as the Appellant suggested. Lord Kerr said that: 'A power on which there are insufficient legal constraints does

[53] For recent overviews of the challenges that algorithmic governance makes to existing legal categories, see Kosta, E. 'Algorithmic state surveillance: Challenging the notion of agency in human rights' (2020) Regulation and Governance <doi:10/ghhv2f> (electronic pre-print); Edwards, L. and Veale, M., 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18 <doi:10/gdxthj>.

not become legal simply because those who may have resort to it exercise self-restraint. It is the *potential* reach of the power rather than its actual use by which its legality must be judged'.[54] The Court instead holds that only the facts of the present case count, and that it is not 'necessary or helpful to consider hypothetical scenarios which may arise in the future'.[55] Respectfully, this is not an answer to Lord Kerr's point. Potentiality is not hypothetical, nor is it the opposite of a fact. Rather it is a quality latent in the arrangement of things in the present. It is already here, included in the facts as they stand. By opposing potentiality to actuality, the Court narrows the epistemological horizon of the law in relation to new technologies and constrains judicial imagination.

[54] *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88 [102].
[55] n 1 above, at [60].