



Know Your Rights: Kettles and Facial Recognition

Maya Sikand, Garden Court Chambers (Chair)

Michael Goold, Garden Court Chambers

Danielle Manson, Garden Court Chambers

Louise Hooper, Garden Court Chambers



GARDEN COURT CHAMBERS



23 June 2020



@gardencourtlaw

Know Your Rights: Kettles and Facial Recognition

Michael Goold, Garden Court Chambers

23 June 2020



GARDEN COURT CHAMBERS



@gardencourtlaw

What is Kettling?

Public order policing tactic.

Also referred to as “containment”, involves detaining a group of (usually) protestors in an area by either surrounding them or blocking their exits from the area with cordons of police officers.

Derives from common law police power to suppress or prevent a breach of the peace.





Breach of the Peace

Howell [1982] QB 416 – a “breach of the peace” is harm actually done or likely to be done to a person or their property or where a person fears being so harmed by public disorder.

Leading case on powers that arise is *Laporte* [2007] 2 AC 105:

Every constable, and also every citizen, enjoys the power and is subject to a duty to seek to prevent, by arrest or other action short of arrest, any breach of the peace occurring in his presence, or any breach of the peace which (having occurred) is likely to be renewed, or any breach of the peace which is about to occur.

Where preventative action is taken because it is feared a BotP is about to occur, there must be a reasonable apprehension that the BotP is “imminent”.

Action can only be taken against innocent parties in order to prevent an imminent breach of the peace only if “there is no other way” to do so.



Kettling: Legal Justification

The leading case is *Austin* [2009] 1 AC 564 (HL); [2008] QB 660 (CA). Police contained thousands in Oxford Circus for several hours, relied on power to prevent breach of the peace.

Innocent people detained so, following *Laporte*, police had to demonstrate that BotP was imminent, and there was no other way to prevent it other than containment.

Court of Appeal imposed following criteria for lawful kettling (see [35]):

- BotP is occurring or reasonably thought to be imminent,
- all other possible steps to stop or prevent BotP that don't impact on rights of innocent people must first be taken,
- proper advance preparations for dealing with any potential BotP were made,
- police reasonably believe that there are no other means of preventing BotP; “this is a test of necessity which is to be expected can only be justified in truly extreme and exceptional circumstances”,
- the action taken is both reasonably necessary and proportionate.



Kettling: Legal Justification (2)

Court of Appeal found those conditions were met in this case, thus the containment was lawful. Notably, Court found that right to liberty under Art. 5 ECHR did not apply as the containment did not amount to a “deprivation of liberty” which would have engaged Art. 5, but rather an “interference with liberty of movement”.

House of Lords and European Court of Human Rights upheld the Court of Appeal’s ruling.

In relation to Art. 5, the House of Lords agreed that it was not engaged by “measures of crowd control”, including containment, so long as they are not “arbitrary”, meaning they must be:

- resorted to in good faith,
- proportionate to the situation which has made the measures necessary,
- enforced for no longer than is reasonable necessary

While all this sounds very strict and exceptional, in practice there has been extremely little success in challenging lawfulness of any kettles.



Kettling for Evidence Gathering?

Clear from *Austin* that the only permissible basis for kettling is prevention or suppression of breach of the peace. Must be necessary, proportionate, in response to exceptional circumstances, the only thing that will work, for as short as possible duration.

Questions around the purpose of kettling arose in the case of ***Mengesha* [2013] EWHC 1695 (Admin)**.

A group of demonstrators were contained after alleged disorder. As they were being released one at a time, each protestor was required to submit to a search, be filmed and provide their name and address, or else they were returned to the containment.

In initial written arguments, the police argued that the requirement to provide details was part and parcel of the containment itself; “a necessary but brief adjunct”. By the time of the hearing, that argument was abandoned and the police accepted there was no power to require personal details “as the price for release”. Instead they argued that the claimant had given her details and submitted to filming voluntarily, an argument the High Court dismissed.



Kettling for Evidence Gathering? (2)

The Court in *Mengesha* found that searching the individuals after they left the containment was lawful, as there was an order under s.60 Criminal Justice and Public Order Act 1994 in force at the time which allowed stop and search without reasonable suspicion.

However, the Court found that the filming and requiring personal details was unlawful. Applying *Laporte* and *Austin*, containment could be maintained only as long as a BotP was imminent and the containment was necessary to prevent it. At the point that the containment was being released in *Mengesha*, the police necessarily no longer believed that a BotP was imminent. Accordingly, extending the duration of the containment in order to obtain individuals' personal details was unlawful.

The film taken of the claimant whilst being released had therefore also been obtained unlawfully and must be destroyed.



S.50 Police Reform Act 2002

Although not relied upon in their defence in *Mengesha*, police at the scene were citing s.50 Police Reform Act 2002 as a requirement for demonstrators to provide their details.

S.50(1) provides:

If a constable in uniform has reason to believe that a person has engaged, or is engaging, in anti-social behaviour, he may require that person to give his name and address to the constable.

It is an offence not to comply with such a request. “Anti-social behaviour” carries the same definition as in other ASB legislation, namely conduct that has caused or is likely to cause harassment, alarm or distress.

It is doubtful that this power applies in public order situations such as arose in *Mengesha*.

First, police would require reason to believe that the individual they were questioning had engaged in ASB. Given the indiscriminate nature of kettling, that is unlikely to be the case.



S.50 Police Reform Act 2002 (2)

Second, it is questionable whether public disorder and the kind of conduct which results in kettling amounts to anti-social behaviour. The language of ASB – harassment, alarm and distress – does feature in certain Public Order legislation, in particular offences under ss. 4A and 5 Public Order Act 1986.

However, the language used in legislation which *regulates* public order situations, such as ss.12 to 14 POA 1986, tends to be of higher level such as serious public disorder, serious damage to property, serious disruption to the life of the community.

The PRA 2002 contained a number of amendments to anti-social behaviour legislation. There is no suggestion in the explanatory notes that it was intended to apply to public order situations.



Current Situation

Police used kettles at recent Black Lives Matters led demonstrations (along with horses, batons and general violence).

It's been reported that they again required individuals to submit to searches under s.60 CJPOA 1994 as they left, *but also* they again required personal details be provided and for individuals to submit to filming by facial recognition cameras. Witnesses reported some police telling demonstrators that “Mengesha rights didn't apply”. Again, police reportedly cited s.50 PRA 2002 as justification for requiring name, address and date of birth (the last of which isn't even covered by s.50).

It may well be that these actions are again subject to legal challenge. In the meantime, this is an indication that the police are intending to use draconian tactics against demonstrators in the current environment.



Know Your Rights: Kettles and Facial Recognition

Danielle Manson, Garden Court Chambers

23 June 2020









GARDEN COURT CHAMBERS



@gardencourtlaw

Live or Automated Facial Recognition technology ('LFR' or 'AFR')

'AFR permits a relatively mundane operation of human observation to be carried out much more quickly, efficiently and extensively. It is technology of the sort that must give pause for thought because of its potential to impact upon privacy rights.'

<p>March 2020</p>				
	<p>Halt public use of facial recognition tech, says equality watchdog</p> <p>Equalities and Human Rights Commission says mass AFR surveillance is discriminatory and stifles free expression</p> <p>● 12 Mar 2020</p>	<p>'Ban this technology': students protest US universities' use of facial recognition</p> <p>Students staged protests on a dozen campuses while 36 schools saw online actions</p> <p>● 3 Mar 2020</p>		
<p>February 2020</p>	 <p>Met police chief: facial recognition technology critics are ill-informed</p> <p>● 24 Feb 2020</p>	 <p>Rules urgently needed to oversee police use of data and AI - report</p> <p>● 23 Feb 2020</p>	 <p>❗ No, Clearview AI's creepy plan to spy on us is not 'free speech' <i>Jake Laperruque</i></p> <p>● 14 Feb 2020</p>	 <p>Watchdog rejects Met's claim that he supported facial recognition</p> <p>● 12 Feb 2020</p>

Live or Automated Facial Recognition technology ('LFR' or 'AFR')

- A 'watchlist' of images of persons of interest is compiled (the police already have explicit statutory powers to acquire, retain and use such imagery: 64A Police and Criminal Evidence Act 1984)
- LFR/AFR technology has a camera which scans the crowd in real time and indicates if a person matches an image on the 'watchlist'
- *'Thus, whilst use of CCTV cameras is a premise for use of AFR, AFR technology goes further. A CCTV camera simply captures digital video recordings. AFR technology uses that digital information to isolate pictures of individual faces, extract information about facial features from those pictures, compare that information with the watchlist information, and indicate matches between faces captured through the CCTV recording and those held on the watchlist.'*
- If there is no match, the facial biometrics/image of the person is deleted
- If there is a match, this is reviewed by a police officer ('the human eye is used to ensure that an intervention is justified') and consequential action will then be taken



Categories of persons on a 'watchlist'

- Persons wanted on warrants;
- Individuals who are unlawfully at large (having escaped from lawful custody);
- Persons suspected of having committed crimes;
- Persons who may be in need of protection (e.g. missing persons);
- Individuals whose presence at a particular event causes particular concern;
- Persons of possible interest for intelligence purposes; and
- Vulnerable persons



Police Powers

- The use of LFR/AFR technology is based on existing police powers under statute and common law
- If an individual is identified using LFR/AFR technology, the particular police powers that are subsequently engaged will depend on the category of the entry on the 'watchlist'
- The technology is not governed by any new dedicated statutory provisions
- The technology is not a form of covert surveillance (were AFR to be used covertly it would be subject to the Regulation of Investigatory Powers Act 2000 'RIPA')
- The police do not have a general right to detain or otherwise deal with persons just because it would help them more readily exercise their functions and discharge their duty to investigate crime



R v Iqbal [2011] EWCA Crim 273

Paragraph 8

'The duty of police officers to bring offenders to justice does not provide them with broad powers which they are entitled to exercise when and how they think it reasonable for them to do so, even if, assuming that they have the powers, it would be reasonable for them to do so. Statutory powers of arrest are granted by the Police and Criminal Evidence Act 1984, as amended by subsequent statutes such as the Police Reform Act 2002 and the Criminal Justice Act 2003, as inserted by the Police and Justice Act 2006. Powers are also granted to stop and search under various different statutes, including the Police and Criminal Evidence Act 1984, the Criminal Justice and Public Order Act 1994 and the Terrorism Act 2000. However, the powers do not extend to a right to detain a citizen because it would help the police more readily to exercise their responsibilities.'

R (Bridges) v Chief Constable of South Wales Police [2019] EWHC 2341 (Admin)

- Leading Case
- Claimant was not on a 'watchlist'
- AFR Locate vs AFR Identify
- Concluded that the use of LFR/AFR technology by South Wales Police was lawful
- Reservations expressed by the Information Commissioner
- Appeal due to be heard today!



South Wales Police ('SWP')

- National lead on use of AFR/LFR technology
- Conducting trials since mid 2017 (first deployment at UEFA Champions League final)
- Secretary of State had been funding the SWP Biometric Strategy
- There is an 'Oversight and Advisory Board' who consider the use of facial images and AFR/LFR technology by law enforcement authorities
- More police forces are now using LFR/AFR technology, including the Met



Bridges: A possible match?

Paragraph 33

'If during a deployment of AFR Locate the software identifies a possible match between a face captured on the CCTV and an image on the watchlist, the two images are reviewed by an AFR operator ('the system operator', who is a police officer) to establish whether he believes that a match has in fact been made. In our view, the fact that human eye is used to ensure that an intervention is justified, is an important safeguard. If, upon reviewing the images of the person on the watchlist and the person whose image has been captured by CCTV, the system operator does not consider that they are the subject of interest, then no further action is taken. If, however, he believes there is a match, he may inform other officers stationed nearby who will intervene ('intervention officers').'



Bridges: Traffic Lights

Paragraph 33 continued...

'SWP have developed a 'traffic light' system with colours (red, amber and green) to delineate the urgency and type of intervention required. 'Red' indicates the need for an immediate response because, e.g., of a counter-terrorist threat, 'amber' indicates the need for an arrest intervention, and 'green' indicates the need for an identification for intelligence development purposes only. If the person identified is on a 'red' watchlist, the system operator may be given instructions to contact the person responsible for the decision that that person should be placed on the watchlist and to obtain instructions as to what action should be taken.'



Bridges: Police Powers

Paragraph 69

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

‘[I]t is part of the obligations and duties of a police constable to take all steps which appear to him necessary for keeping the peace, for preventing crime or for protecting property from criminal damage. There is no exhaustive definition of the powers and obligations of the police, but they are at least those, and they would further include the duty to detect crime and to bring an offender to justice.’



Bridges: Police Powers

Paragraph 70

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



Bridges: Police Powers

Paragraph 71

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

'At common law the police have the power to obtain and store information for policing purposes, i.e. broadly speaking for the maintenance of public order and the prevention and detection of crime. These powers do not authorize intrusive methods of obtaining information, such as entry onto private property or acts (other than arrest under common law powers) which would constitute an assault. But they were amply sufficient to authorize the obtaining and storage of the kind of public information in question on these appeals.'



Bridges: Police Powers

Paragraph 72

'Third, the police may make reasonable use of a photograph of an individual for the purpose of the prevention and detection of crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large and may do so whether or not the photograph is of any person they seek to arrest or of a suspected accomplice or of anyone else.'

'The key is that they must have these and only these purposes in mind and must ...make no more than reasonable use of the picture in seeking to accomplish them' (per Laws J in Hellewell v Chief Constable of Derbyshire [1995] 1 W.L.R. 804 at 810F).'



Bridges: Police Powers

Paragraph 73

'It will be apparent from the passages highlighted in the judgments in Rice and Catt, that the extent of the police's common law powers has generally been expressed in very broad terms. The police did not need statutory powers, e.g. to use CCTV or use body-worn video or traffic or ANPR16 cameras, precisely because these powers were always available to them at common law. Specific statutory powers were needed for e.g. the taking of fingerprints, and DNA swabs to obviate what would otherwise be an assault.'



In summary...

- The police are permitted to photograph people as they go about their business *R(Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123 and *R(Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9) which (as it stands) extends to the deployment of LFR/AFR technology
- However, there is no specific police power to take images of a persons face and/or no legal duty for a person to make their face available for images to be taken by police unless and until the threshold for arrest is met
- If someone is identified by virtue of LFR/AFR whether the police can exercise their ordinary powers of arrest will depend on all the circumstances and the factual scenario, namely the category of the 'watchlist' the individual falls within and/or whether the police have reasonable grounds etc.



‘The protection afforded by art.8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.’

S v United Kingdom [2009] 48 EHRR 50



Know Your Rights: Kettles and Facial Recognition

Louise Hooper, Garden Court Chambers

23 June 2020



GARDEN COURT CHAMBERS



@gardencourtlaw

Louise Hooper,
Garden Court Chambers

23 June 2020

1984
WAS

NOT

SUPPOSED
TO BE AN
INSTRUCTION
MANUAL

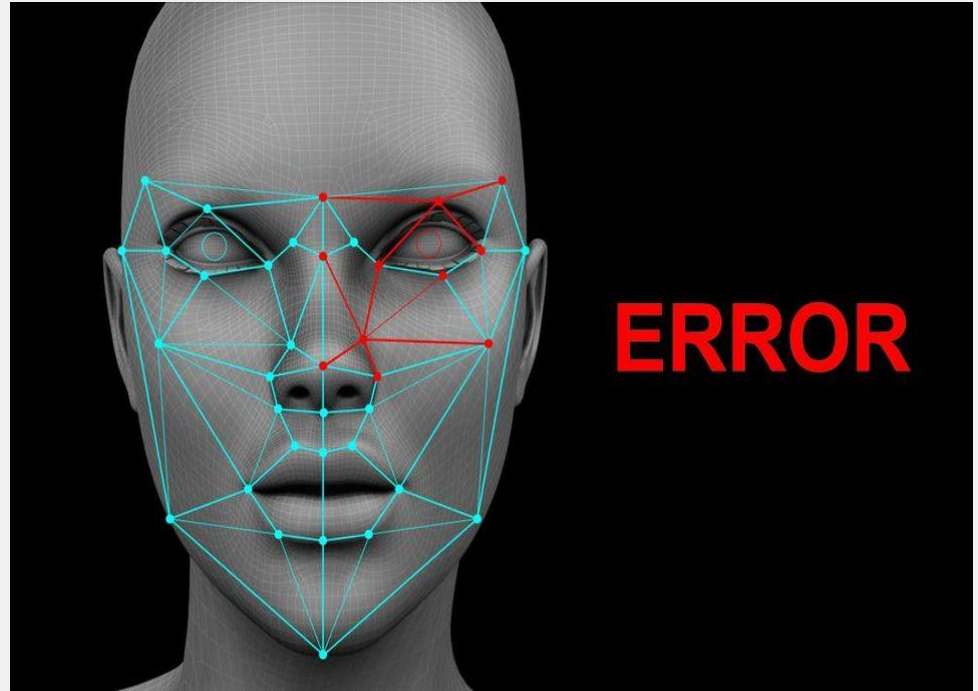
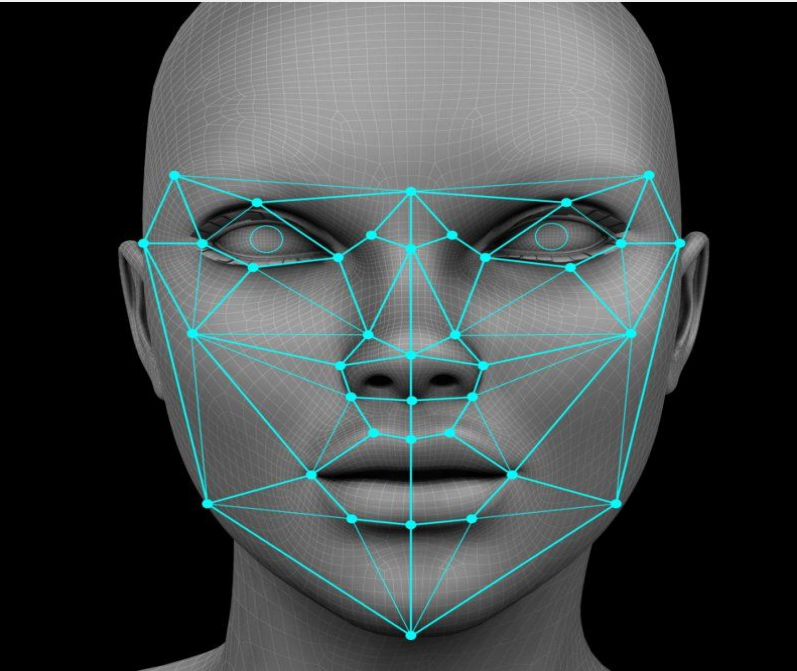




Images of me and others at protests taken from publicly available sources



LFR: How does it work?



shutterstock




















Training data: Chihuahua or muffin?



https://cdn-media-1.freecodecamp.org/images/1*bt-E2YcPafjiPbZFDMmNQ.jpeg

Gender Shades Research, Joy Buloamwini et al

Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
 Microsoft	94.0% 	79.2% 	100% 	98.3% 	20.8% 
 FACE++	99.3% 	65.5% 	99.2% 	94.0% 	33.8% 
IBM	88.0% 	65.3% 	99.7% 	92.9% 	34.4% 



<http://gendershades.org/overview.html>



IBM will no longer offer, develop, or research facial recognition technology

IBM's CEO says we should reevaluate selling the technology to law enforcement

By Jay Peters | @jaypeters | Jun 8, 2020, 8:49pm EDT

f   SHARE



GOOD DEALS



Save \$50 on Eero's three-pack of mesh Wi-Fi routers and get a free Echo Dot



Amazon bans police from using its facial recognition technology for the next year

The product, called Rekognition, has been the source of controversy

By Nick Statt | @nickstatt | Jun 10, 2020, 5:37pm EDT

f   SHARE

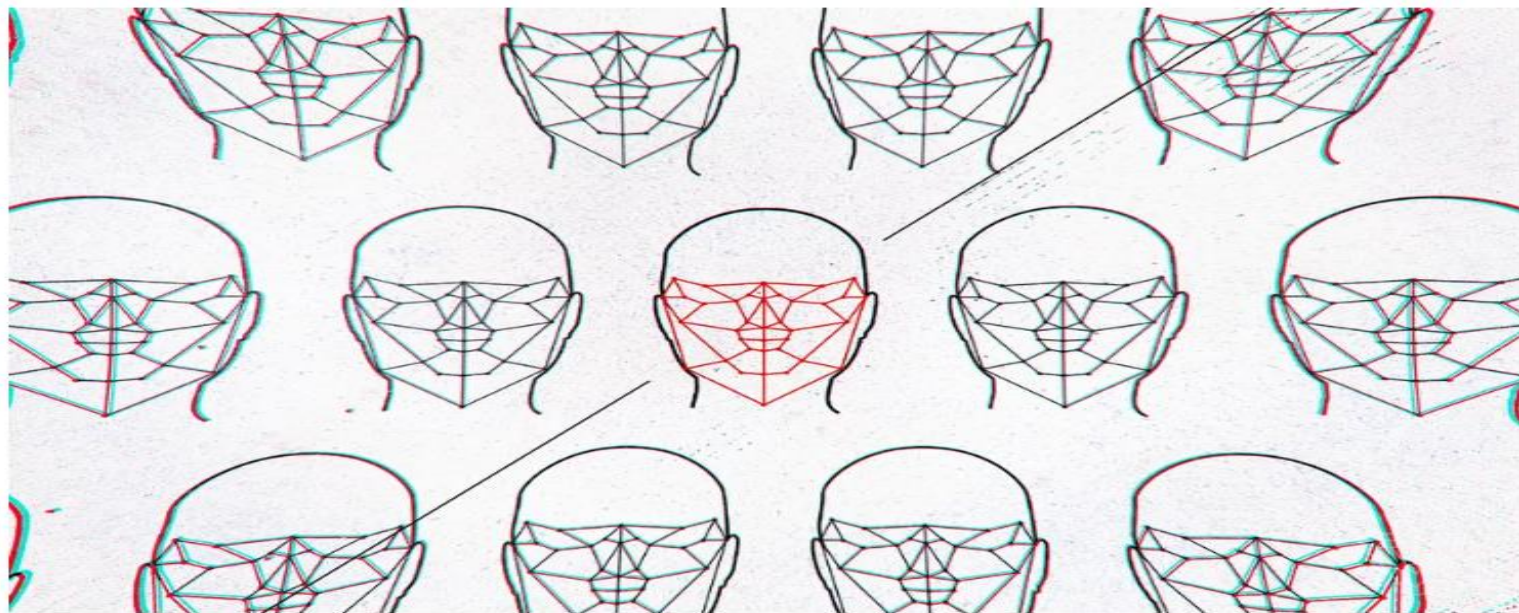


Illustration by Alex Castro / The Verge

Amazon is announcing a one-year moratorium on allowing law enforcement to use its controversial Rekognition facial recognition platform, the [e-commerce giant said on Wednesday](#).

Microsoft's Brad Smith says company will not sell facial recognition tech to police

Anthony Ha @anthonyha / 6:39 pm BST • June 11, 2020

Comment



Where is the UK?

- SWP in court defending lower court decision in *Bridges* that the interference with the right to privacy is necessary and proportionate.
- MPS rolling out use of LFR across London
- Government committed to more and more investment in AI and tech
- AI Procurement in a Box- good step forwards...but query application?



Watchlist data

- *Bridges 105: ‘The inclusion of any person on any watchlist and the consequent processing of that person’s personal data without sufficient reason would most likely amount to an unlawful interference with their own Article 8 rights’*
- MPS guidance
 - Inclusion on list must be necessary and proportionate and meet identified policing purpose
 - Limited in size to meet the policing purpose AND to ensure alerts can be managed
- Criticisms have been made of the composition of watchlists by the ICO:
 - Insufficiently targeted
 - Uses custody images database which has serious flaws including the unlawful retention of images that should have been destroyed= unlawfully held images used to compile watchlists
 - unspecified other sources including ‘social media’ (see ICO investigation into MPS Gangs Violence Matrix)
 - Unspecified other sources including ‘social media’
 - Lack of guidance on accuracy or sources



Reliability:

- During 55 hours of deployment the system flagged up 2,900 potential matches of which 2,755 were false positives. The police made 18 arrests using the system, but the Cardiff report does not state whether any of the individuals were charged.
- The Welsh trial highlighted another challenge for facial recognition: lambs. Not farmyard fugitives but people on the watchlist who happen look like plenty of other people. While scanning the crowds at Welsh rugby matches, the NeoFace system spotted one woman on the South Wales police watch list 10 times. None of them were her.
<https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it>



LOUISE HOOPER > GARDEN COURT CHAMBERS > LONDON, ENGLAND > LAWYER PROFILE

GARDEN COURT CHAMBERS OFFICES

London



GARDEN COURT CHAMBERS
GARDEN COURT CHAMBERS
57-60 LINCOLN'S INN FIELDS
LONDON
WC2A 3LJ
ENGLAND

FIRM PROFILE GO TO... Position Lawyer Rankings

LOUISE HOOPER



020 7993 7600
info@gclaw.co.uk

Position

<http://www.gardencourtchambers.co.uk/barrister/louise-hooper/>

Lawyer Rankings

About 254 results (0.79 seconds)



Image size:
140 × 210

No other sizes of this image found.

Possible related search: [woman](#)

[en.wikipedia.org](#) > [wiki](#) > [Woman](#) ▾

Woman - Wikipedia

A **woman** is a female human being. The word **woman** is usually reserved for an adult; girl is the usual term for a female child or adolescent. The plural women is ...

[www.dictionary.com](#) > [browse](#) > [woman](#) ▾

Woman | Definition of Woman at Dictionary.com

Woman definition, the female human being, as distinguished from a girl or a man. See more.

Visually similar images



[Report images](#)

Woman



A woman is a female human being. The word woman is usually reserved for an adult; girl is the usual term for a female child or adolescent. The plural women is also sometimes used for female humans, regardless of age, as in phrases such as "women's rights".
[Wikipedia](#)

[Feedback](#)



Home

Explore

Notifications

Messages

Bookmarks

Lists

Profile

More

Tweet



Louise Hooper

3,759 Tweets



Edit profile

Louise Hooper

@Louise1Hooper

Barrister, Garden Court Chambers. Feminist. She/Her. Law: Human Rights, Equality, Refugees, Gender, Tech. Non-law: Mountains, Cats, Bicycles. Views my own

Joined October 2014

790 Following 990 Followers

Tweets

Tweets & replies

Media

Likes

Pinned Tweet



Louise Hooper @Louise1Hooper · Nov 24, 2017

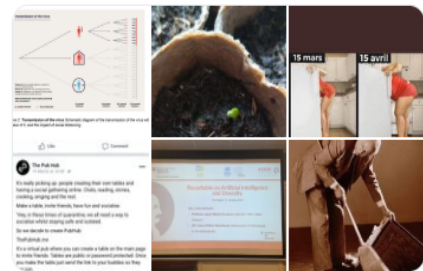
#ViolenceAgainstWomen #IstanbulConvention free #elearning course now available.



Eva Pastrana @evapastrana3 · Nov 24, 2017

New HELP #elearning course against #ViolenceAgainstWomen available in help.elearning.ext.coe.int The course was presented at @Europarl_EN Parliament by libe @EP_GenderEqual Committee. Watch (9 min) from 15:29:10' at web.ep.streamovations.be/index.php/even...

Search Twitter



You might like



Shoab M Khan @ShoabMKhan

Follow



Bell Ribeiro-Addy @BellRibeiroAddy

Follow

Show more

What's happening

UK news · Earlier today

Remembering the Windrush generation on the 72nd anniversary of the ship's arrival



Pop · Trending

Liam Payne 43.5K Tweets

Trending in United Kingdom

#boycotttheBodyShop



Image size:
400 × 400

Find other sizes of this image:
All sizes - Medium

Possible related search: **man**

www.mantruckandbus.com > ... ▾

MAN as a company — MAN Truck & Bus

MAN Truck & Bus: find out everything about **MAN** and our products. Discover exciting stories, videos & interviews about commercial vehicles & transport ...

www.corporate.man.eu > ... ▾

MAN Group | MAN SE

MAN supplies trucks, buses, diesel engines and turbomachinery as well as turnkey power plants. **MAN's** divisions hold leading positions in their respective ...

Visually similar images



Report images

Man



A man is an adult male human. Prior to adulthood, a male human is referred to as a boy. Like most other male mammals, a man's genome typically inherits an X chromosome from his mother and a Y chromosome from his father. [Wikipedia](#)

Feedback

Private Life?

YES

- Private life includes physical and psychological integrity of a person/social identity. Includes gender, name, other means of personal identification and of linking to a family, ethnic identity, and elements relating to a person's right to their image *S v UK* (2009) 48 EHRR 50 [66]
- Facial biometric information is 'a unique identifier'
- Distinguished between taking a photo (*see R(Wood) v Commissioner of the Police of the Metropolis* [2010] 1 WLR 123 and AFR locate on grounds:
 - Image is taken
 - Digital information is then analysed and the biometric facial data is extracted
 - That information is then processed in the sense that it is compared to a watchlist
- Private life is therefore engaged



Interference?

YES

- Private life can be infringed in a public space. This has been held to occur where a ‘systematic or permanent record comes into existence of [monitoring material] from the public domain’ *PG v United Kingdom* (2008) 46 EHRR
- Storing of data relating to private life *per se* amounts to an interference with art 8 irrespective of what use is made of it (*S and Marber v UK* @ 67)
- *Bridges*@ 59-60 Article 8 is triggered by the initial gathering of the information. *‘The fact that the process involves the near instantaneous processing and discarding of a person’s biometric data where there is no match with anyone on the watchlist (and such data is never seen by or available to a human agent) does not matter.’*



Extent of the interference?

Query- What constitutes the interference? The existence of the system? The comparison with a watchlist? The impact on the behaviour of an individual or a group? The Court does not seem to address the fact of surveillance or the societal consequences just the results for an individual after the event

- *Bridges Para 7:*

‘AFR is another **new and powerful technology**...Its use by public authorities also gives rise to **significant civil liberties concerns**. Using AFR can involve processing the facial biometric data of large numbers of people. The **raw power of AFR-** and the **potential baleful uses** to which AFR could be put by agents of the state and others underline the need for careful and on-going consideration of the effectiveness of that [legal] framework...’

- *@61* Accept that for all people (not just those on a wanted list)

‘the use of **AFR**...in crowded places and selected sites will **significantly enhance** the capabilities of a surveillance camera **system to intrude and gather private information of a citizen**.



Extent of the interference 2?

- *Bridges* para 75: Court held that there was no ‘intrusive act’:
...‘No physical entry, contact or force is necessary when using AFR Locate to obtain biometric data. It simply involves taking a photograph of someone’s face and the use of algorithms to attempt to match it with photographic images of faces on a watchlist. The method is no more intrusive than the use of CCTV in the streets’
- @101
‘The interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant’s biometric data.’
- No consideration of the wider consequence of the interference on groups, behaviour, indirect impact on other freedoms such as freedom of association, assembly, expression, movement, discrimination. Potential for stigmatisation arising from false positives- see *S and Marper v UK @122* (there in the context of retained data)



Terror police list that included Extinction Rebellion was shared across government

Document was sent to several departments, NHS England, Ofsted and 20 councils

Jamie Grierson and Vikram Dodd

Mon 27 Jan 2020 14:13 GMT



▲ The Extinction Rebellion flag in Marble Arch, London, last year. Photograph: Nick Moore/Alamy Stock Photo

Controversial guidance that listed **Extinction Rebellion** as an extremist ideology was sent to a wide range of government departments and local authorities including the Home Office and Counter Terrorism Policing headquarters, the Guardian can reveal.

Legitimate Aim?

YES

- *Bridges at 99* Not disputed that SWP uses AFR locate for a legitimate aim that is also sufficiently important to justify the interference
- Too wide?
 - ECHR noted ‘the objective of prevention or detection of crime ‘is worded in rather general terms and may give rise to extensive interpretation’ *S and Marper v UK* at [99]
 - All crime?
 - Some crime?
- See also *Weber and Saravia v Germany* App No 54934/00, 29 June 2006 [103-104] and *R(on the application of Roberts)(Appellant) v Commissioner of Police for the Metropolis and anr (Respondents)* [2015] UKSC 79 [3]



Necessary?

YES

- In *Bridges* the Court recognises the need under Art 8 for the interference to be necessary and under the DPA to be ‘strictly necessary’ but relied on the proportionality assessment to find that it was necessary [98-106, 127, 136]
- At 127 ‘*the processing is necessary for SWP’s legitimate interests taking into account of the common law obligation to prevent and detect crime*’



What/Why/How necessary?

- To identify individuals wanted by the Courts and police
 - Wanted for what? Theft? Terrorism?
 - How serious is the intelligence?
 - Data is dirty- includes people no longer wanted
- Individuals who present a risk of harm to themselves and others
 - Define harm?
- To support ongoing police activity with regards a specific problem/location
- To assist police in identifying individuals who may be at risk or vulnerable

- Is the technology sufficiently accurate and reliable to be 'necessary'?
- Is it necessary to include X on the watchlist?
 - What is the nature of the crime they are suspected of?
 - What is the nature of their inclusion at all?
- Is it necessary to deploy at all?
 - What is the nature of the crime police seek to prevent
- Is it necessary to deploy in that location?



Proportionate?

YES

- The **objective pursued must be proportionate to the seriousness of the interference**- see *Watson* there in context of covert surveillance where only the objective of fighting ‘serious crime’ was capable of justifying access to retained data
- Serious crime: threats to national security and activities that will affect the monetary stability of the state (*Rechnungshof v Osterreichischer Rundfunk and others C-465/00, C-138/01 and C-139/01*)



Proportionate?

- *Bridges* at 101:

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



Equality Act 2010, s149 PSED, Article 14 ECHR

- Dissenting judgment of Kerr L in *Beghal v DPP* [2015] UKSC 49: The opportunity to exercise a coercive power in an arbitrary or discriminatory fashion is antithetical to its legality.’ (cited at [3] of *Roberts*)
- *Bridges at 153 and 156* Court held no reasons in April 2017 that SWP should or ought to have recognised the potential for discrimination...
- Review in light of Gender Shades? Review in light of announcements by IBM, Microsoft, Amazon?
- Impact of existence of discrimination on ‘in accordance with the law’ or ‘legitimate aim’?
- Discrimination in compilation of watchlist? See e.g. The Lammy Report
- Future issues: Discrimination in location of LFR? (see e.g. Essex University report references to Westfield Shopping centre rather than the areas of Stratford where crime actually existed)



What next?

- Automated inference on criminality using face images: <https://arxiv.org/pdf/1611.04135v1.pdf>
- Use of social media to impute political view? https://cnets.indiana.edu/wp-content/uploads/conover_prediction_socialcom_pdfexpress_ok_version.pdf
- Predictive analytics: replicate and amplify pre-existing bias? <https://www.theguardian.com/uk-news/2019/sep/16/predictive-policing-poses-discrimination-risk-thinktank-warns>
- https://rusi.org/sites/default/files/20190916_data_analytics_and_algorithmic_bias_in_policing_web.pdf





Images of me and others at protests taken from publicly available sources



RESOURCES



Legislative Framework

- Human Rights Act 1998- query whether just article 8? Liberty have noted that the deployment of this technology causes people to change their behaviour in terms of who they associate with and where they go. (association/movement/expression) Discrimination
- Equality Act 2010, s149 Public Sector Equality Duty
- Data Protection Act 1998
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- The Law Enforcement Directive



Codes and Guidance

- Secretary of State's Surveillance Camera Code of Practice
- Surveillance Camera Commissioner's AFR Guidance
- Data Protection impact assessment guidance (surveillance cameras or surveillance systems) SCC
- In *Bridges*
 - SWP Policy document
 - SWP Standard Operating Procedures
 - SWP Operational Advice



Surveillance Camera Commissioner

- Surveillance camera code of practice: : <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>
- Use of facial recognition technology by South Wales Police, policy paper: <https://www.gov.uk/government/publications/the-use-of-facial-recognition-technology-by-south-wales-police>
- Data protection impact assessments for surveillance cameras: <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras>



Information Commissioner

- Has raised concerns that:
 - LFR involves large scale and relatively indiscriminate processing
 - If not subject to appropriate safeguards could result in ‘serious interference’ with privacy rights
 - There is an absence of national level coordination in assessing privacy risks and a lack of comprehensive framework to oversee AFR deployment
- ICO Opinion: The use of live facial recognition technology by law enforcement in public places, 31 October 2019: <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf>
- ICO investigation into how the police use facial recognition technology in public places, 31 October 2019: <https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf>
- Statement of 24 January 2020 in response to announcement of MPS that will use LFR



Metropolitan Police

- <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/>
- Has links to
 - Law and legislation
 - Live facial recognition legal mandate
 - LFR Standard Operating Procedures
 - LFR Guidance Document
 - NPIA – Capture and interchange for facial and SMT images
 - Data Protection Impact Assessment
 - Equality Impact assessment
 - How we're complying with the surveillance camera code of practice
 - Appropriate policy document
- London Policing Ethics Panel: Final Report on Live Facial Recognition, May 2019:
http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf



Other resources:

- Liberty: <https://www.libertyhumanrights.org.uk/issues/?scroll-to=topics&subtopic-filter=privacy-and-mass-surveillance-facialrecognition&topic-filter=privacy-and-mass-surveillance>
- University of Essex, Human Rights, Big Data and Technology report <https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns>
- Centre for Data Ethics and Innovation: <https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology>
- Ada Lovelace Institute: <https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/>
- Privacy International: <https://privacyinternational.org/learn/facial-recognition>
- Big Brother Watch: <https://bigbrotherwatch.org.uk/> (in particular: <https://bigbrotherwatch.org.uk/wp-content/uploads/2019/06/Big-Brother-Watch-submission-to-the-Centre-for-Data-Ethics-and-Innovation-Bias-in-Algorithmic-Decision-Making-Crime-and-Justice-June-2019.pdf>)



Thank you

020 7993 7600

info@gclaw.co.uk

@gardencourtlaw

