FACE OFF

The lawless growth of facial recognition in UK policing

May 2018

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk
@bbw1984

About Big Brother Watch

Big Brother Watch exposes and challenges threats to our privacy, our freedoms and our civil liberties at a time of enormous technological change in the UK.

We work to roll back the surveillance state and protect the rights of everyone in the UK to be free from unfair intrusion.

We campaign to protect freedoms in Parliament and through the courts. We produce unique research and investigations, and seek to educate and empower the public.

Big Brother Watch is a cross-party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK.

In our pursuit for change, we use advocacy and campaigns; parliamentary lobbying; public interest litigation; research and investigations that inform policy and public debate; and public education and empowerment.

Contact

Silkie Carlo
Director
Email: silkie.carlo@bigbrotherwatch.org.uk

Jennifer Krueckeberg
Lead Researcher
Email: jennifer.krueckeberg@bigbrotherwatch.org.uk

Griff Ferris
Legal and Policy Officer
Email: griff.ferris@bigbrotherwatch.org.uk

24hr media line: 07505 448925

www.bigbrotherwatch.org.uk

Contents

Executive Summary	1
How does facial recognition technology work?	5
Beyond the rule of law	9
The threat to fundamental rights	13
Contribution from Samir Jeraj, Race Equality Foundation	17
Facial recognition and the unlawful retention of custody images in the UK	21
Automated facial recognition and law enforcement in the UK	25
Resistance to facial recognition around the world	35
Contribution from Jay Stanley, ACLU	38
Contribution from Clare Garvie, Georgetown Law	39
Contribution from Jennifer Lynch, EFF	40
Conclusion	41

Executive Summary

Facial recognition has long been feared as a feature of a future authoritarian society, with its potential to turn CCTV cameras into identity checkpoints, creating a world where citizens are intensively watched and tracked.

However, facial recognition is now a reality in the UK – despite the lack of any legal basis or parliamentary scrutiny, and despite the significant concerns raised by rights and race equality groups. This new technology poses an unprecedented threat to citizens' privacy and civil liberties, and could fundamentally undermine the rights we enjoy in public spaces.

Police forces in the UK have rolled out automatic facial recognition at a pace unlike any other democratic nation in the world. Leicestershire Police, South Wales Police and the Metropolitan Police have deployed this technology at shopping centres, festivals, sports events, concerts, community events – and even a peaceful demonstration. One police force even used the surveillance tool to keep innocent people with mental health issues away from a public event.

In this report, we explain how facial recognition technology works, how it is being used by police in the UK, and how it risks reshaping our rights. We are seeking to raise awareness of this growing issue with parliamentarians and inform the wider public about what is happening behind the cameras. In this report, we:

- Reveal new statistics following a series of freedom of information requests, exposing the shocking inaccuracy and likely unlawful practices within a number of police forces using automated facial recognition;
- Analyse the legal and human rights implications of the police's use of facial recognition in the UK;
- Review the evidence that facial recognition algorithms often disproportionately misidentify minority ethnic groups and women;

- Present guest contributions from allies worldwide warning about the impact of facial recognition on rights, including contributions from representatives of American Civil Liberties Union, Electronic Frontier Foundation, Georgetown Privacy Centre, and the Race Equality Foundation;

We conclude by launching our campaign against the lawless growth of facial recognition in the UK, supported by rights groups, race equality groups, technologists, lawyers and parliamentarians.

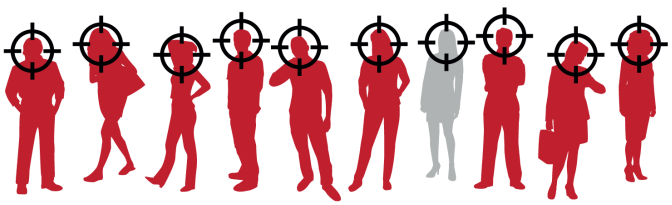
Key Findings

Big Brother Watch's freedom of information-based investigation, involving over 50 requests for information, reveals that:

- The overwhelming majority of the police's 'matches' using automated facial recognition to date have been inaccurate. On average, a staggering 95% of 'matches' wrongly identified innocent people.
- Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

Metropolitan Police

- The Metropolitan Police has the worst record, with less than 2% accuracy of its automated facial recognition 'matches' and over 98% of matches wrongly identifying innocent members of the public.



98% **of automated facial recognition matches by the Met**

wrongly identified innocent people

- The force has only correctly identified 2 people using the technology – neither of which was a wanted criminal. One of those people matched was incorrectly on the watch list; the other was on a mental health-related watch list. However, 102 innocent members of the public were incorrectly identified by automated facial recognition.

- The force has made no arrests using automated facial recognition.

South Wales Police

- South Wales Police's record is hardly better, with only 9% accuracy of its matches whilst 91% of matches wrongly captured innocent people.

- 0.005% of 'matches' led to arrests, numbering 15 in total.

- However, at least twice as many innocent people have been significantly affected, with police staging interventions with 31 innocent members of the public incorrectly identified by the system who were then asked to prove their identity and thus their innocence.

- The force has stored biometric photos of all 2,451 innocent people wrongly identified by the system for 12 months in a policy that is likely to be unlawful.

- Despite this, South Wales Police has used automated facial recognition at 18 public places in the past 11 months – including at a peaceful demonstration outside an arms fair.

Custody images

- Out of the 35 police forces that responded to our Freedom of Information request, not one was able to tell us how many photos they hold of innocent people in their custody image database.

How does facial recognition technology work?

Facial recognition technology measures and matches unique facial characteristics for the purposes of biometric surveillance or identification. Police forces in the UK are currently using two different types of facial recognition:

- Facial Matching: this is the matching of an isolated, still image of an individual against a database of images. For example, a photograph or a still image from surveillance camera footage can be compared against mugshots on the Police National Database.

- Automated Facial Recognition: this is a relatively new technology, in which facial recognition-linked cameras scan crowds and public spaces in attempt to identify people in real-time, by matching faces against a database. The face of each and every person passing by an automated facial recognition camera will be scanned and analysed, effectively subjecting every person within view to a biometric identity check.

> ***Facial recognition technology aims to identify individuals or authenticate individuals by comparing their faces against a database of known faces and looking for a match.***
>
> ***The process can be broken down into three very general steps.***
>
> ***First, the computer must find the face in the image.***
>
> ***It then creates a numeric representation of the face based on the relevant position, size and shape of facial features.***
>
> ***Finally, this numeric map of the face in the image is compared to a database of images of identifies faces.***
>
> \- South Wales Police

Facial recognition software measures facial characteristics to create a unique facial map in the form of a numerical code. The algorithm then compares these measurements to hundreds, thousands, or even millions of other facial images held on a database to find a match.

It is important to note that facial recognition is based on a percentage of corresponding features producing the likelihood of a match, rather than a binary 'yes' or 'no' result.[1]

Many facial recognition technologies are artificial intelligence (AI) systems that learn from the millions of faces they process in order to improve the accuracy of their matches over time. The Metropolitan Police and South Wales Police are using an AI facial recognition product called 'NeoFace Watch' made by Japanese company NEC.

True-positive match

A true-positive match is when a facial recognition system **correctly** matches a person's face with an image held on a database.

False-positive match

A false-positive match is when facial recognition **incorrectly** matches the wrong person's face with an image of another person held on a database.

Faces are the most visible part of our bodies. In contrast to fingerprints or DNA, automated facial recognition technology does not require any physical contact or human engagement to identify an individual, which means most people subjected to these identity checks are not even aware of it.[3]

NEC views the "*non-contact process*" as offering "*distinct advantages*":

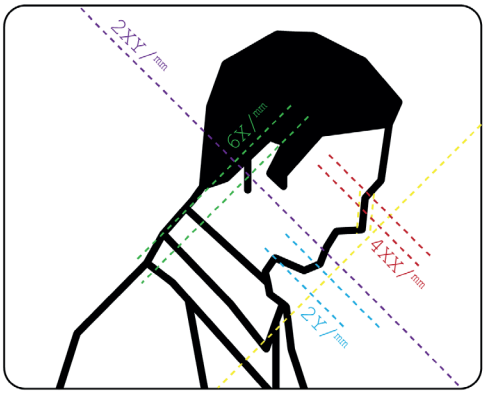
> ***"As compared with other biometrics systems using fingerprint/palmprint and iris, face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person."***[4]

When automated facial recognition is used in real-time in public spaces, law abiding citizens are effectively asked for their papers without their consent or awareness. In our experience, most members of the public have not even heard of automated facial recognition and are not aware of its implications.

How facial recognition works[2]

1. Detection

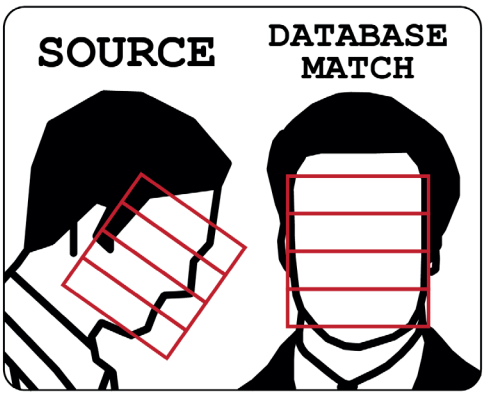
2. Alignment



3. Measurement

4. Representation

5. Matching



6. Verification/indentification

Beyond the rule of the law

Automated facial recognition technology is currently used by UK police forces without a clear legal basis, oversight or governmental strategy, despite its potential to infringe on civil liberties and fundamental rights.

No legal basis

In answer to a Written Parliamentary Question from Layla Moran MP, asking about current legislation regulating *"the use of CCTV cameras with facial recognition and biometric tracking capabilities"*, Nick Hurd MP (Minister of State for Policing, responding for the Home Office) answered: *"There is no legislation regulating the use of CCTV cameras with facial recognition".*[5]

The Surveillance Camera Commissioner has also raised the issue of the lack of a clear statutory footing for facial recognition.[6]

The lack of a legal basis or indeed parliamentary scrutiny poses serious concerns about the silent erosion of human rights. It is highly questionable whether the use of automated facial recognition with public surveillance cameras, scanning and biometrically analysing every passer-by's face, and enabling authorities to identify and track citizens without their knowledge, is compatible with fundamental human rights – in particular, the rights to a private life and to freedom of expression. The necessity of such biometric surveillance is highly questionable, and inherently indiscriminate scanning appears to be plainly disproportionate. As it stands, the risk that automated facial recognition is fundamentally incompatible with people's rights under the Human Rights Act 1998 is yet to be considered.

> ***There is no legislation regulating the use of CCTV cameras with facial recognition***
>
> - Nick Hurd, Minister for Policing – September 2017

No oversight

Accordingly, there has been no formal, independent oversight of the police's use of automated facial recognition in the UK. In 2016, the Surveillance Camera Commissioner raised this concern in his Review on the Surveillance Camera Code of Practice."[7]

Meanwhile the Government has broadly allowed the police to oversee and regulate their own use of this intrusive surveillance and identification technology, announcing that "*A decision to deploy facial recognition systems is an operational one for the police.*" [8]

However, following pressure from NGOs and parliamentarians, Baroness Williams (Minister of State for Countering Extremism) wrote to the Chair of the Science and Technology Committee in March 2018 stating that Government intends to "*improve independent oversight and governance*" by setting up an automated facial recognition "board" including the Surveillance Camera Commissioner, the Biometrics Commissioner, the Information Commissioner and police representatives.[9] The Minister added the board will "*provide greater assurance that policing is complying with guidance*", but it is unclear what 'guidance' she is referring to. There is no formal guidance or policy on police use of facial recognition.

In fact, it is unprecedented for government to provide a board to provide 'guidance' on the use of a policing power that is being deployed ultra vires.

No policy

The Government said that the Home Office would publish a 'Forensics and Biometrics Strategy' by 2013, but failed to. The Home Office eventually published a strategy three years late in March 2016 that only covered forensics.

Despite several missed deadlines and its failure to publish a Biometrics Strategy, our investigation shows that the Home Office has awarded South Wales Police a total of £2.6m from the 'Police Innovation Fund' and 'Home Office Biometrics' to take a national lead in deploying automated facial recognition.[10]

Five years later and following pressure from NGOs and parliamentarians, the Government has now vowed to produce a 'Biometrics Strategy' in June 2018. It is expected to address automated facial recognition. It remains to be seen whether the Government will adhere to its own deadline this time.

By contrast, the Scottish Government commissioned and subsequently published a review of its use of biometrics, including facial matching and the retention of custody images, in under a year.[11]

We call on UK public authorities to immediately stop using automated facial recognition software with surveillance cameras.

The threat to fundamental rights

A threat to the right to privacy

Live automated facial recognition cameras, acting as biometric identification checkpoints, are a clear threat to both individual privacy and privacy as a social norm.

The Human Rights Act 1998 requires that any interference with the Article 8 right to a private life is both necessary and proportionate. However, the use of automated facial recognition with CCTV cameras in public spaces appears to fail both of these tests.

Automated facial recognition cameras scan the faces of every person that walks within the view of the camera; the system creates, even if transitorily, a biometric scan of every viewable person's face; it compares those biometric scans to a database of images; and it retains photos of all individuals 'matched' by the system, despite 95% of matches inaccurately identifying innocent people. As such, automated facial recognition cameras are biometric identification checkpoints that risk making members of the public walking ID cards.

It is plainly disproportionate to deploy a technology by which the face of every passer-by is analysed, mapped and their identity checked. Furthermore, a facial recognition match can result in an individual being stopped in the street by the police and asked to prove their identity and thus their innocence.

Members of the public who have been scanned by automated facial recognition are unlikely to be aware that they were subject to the identity check, and do not have a choice to consent to its use. The Biometrics Commissioner commented: *"(...)unlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge."*[12] In a recent question for short debate in the House of Lords on the use of facial recognition in security and policing – incidentally, the first parliamentary debate on the topic, tabled by backbencher Baroness Jones of Moulsecoombe – the Lord Bishop of St Albans remarked:

> *"I have taken the trouble to talk to a number of people over the last week to ask them of their awareness of this technology.*

I was very struck by the fact that hardly anybody I spoke to realised what was already going on. Some were horrified, some were puzzled and every one of them had questions and worries."[13]

Proportionality is a particular concern in relation to automated facial recognition due to the general and indiscriminate nature in which the camera biometrically scans the public, often without their knowledge and always without their consent or indeed any objective evidence of wrongdoing. This concern is significantly heightened in the context of the authorities' intentions for the technology. South Wales Police has indicated that it intends to implement automated facial recognition in future throughout the enormous existing CCTV network:

> ***"The technology can also enhance our existing CCTV network in the future by extracting faces in real time and instantaneously matching them against a watch list of individuals."***[14]

A threat to the right to freedom of expression

The right to go about your daily activity undisturbed by state authorities, to go where you want and with whom, and to attend events, festivals and demonstrations, is a core principle of a democratic society protected by Article 10 of the Human Rights Act 1998.

The biometric surveillance and identification of individuals in public spaces and at public events, in particular political demonstrations, is clearly incompatible with that fundamental right.

We are concerned that the use of automated facial recognition with CCTV has a chilling effect on people's attendance of public spaces and events, and therefore their ability to express ideas and opinions and communicate with others in those spaces.

Many of our supporters and those we work with would not be comfortable going to an event if doing so meant being subjected to biometric surveillance. In Scotland, where facial recognition was proposed to be introduced at football grounds in 2016, there was significant opposition, a stadium protest, and concern that the move could "*drive punters away*". Several supporter groups made clear the chilling effect it would have, with one stating that facial recognition cameras would result in "*empty stands*".[15]

Many of the people Big Brother Watch, StopWatch, and Liberty spoke to at Notting Hill Carnival 2017, where automated facial recognition was in use, were shocked and felt both uncomfortable and targeted.

When the Metropolitan Police used the technology at Remembrance Sunday 2017 to identify and eject individuals on a mental health-related watch list, those individual's right to free expression was directly under attack.

We were extremely concerned to learn that South Wales Police recently used automated facial recognition at a lawful and peaceful demonstration outside an arms fair. In the online discourse around the event, we witness the chilling effect this had on demonstrators who expressed that they felt unfairly targeted and surveilled.

If this technology is allowed to continue being used unchecked, it will have a serious and severe chilling effect on the right of freedom of expression in the UK.

A threat to the right to freedom from discrimination

Our investigation reveals that automated facial recognition used by police in the UK is astoundingly inaccurate, with matches averaging 95% inaccuracy. Such misidentifications, in the context of law enforcement, can have serious consequences for people and are likely to disproportionately affect black and minority ethnic groups.

South Wales Police has indiscriminately stored biometric photos of 2,451 innocent people for a year and even staged interventions with 31 innocent people – twice as many people as the suspects they have arrested using the technology - asking them to prove their identity and thus their innocence.

At the time of writing, the Metropolitan Police has refused to disclose full statistics but has told us of 102 people wrongly identified by their system whose biometric photos were stored for 30 days. Officers operating the force's facial recognition software told us at Notting Hill Carnival 2017 they had staged interventions with around 5 innocent people incorrectly matched on one day alone, asking the innocent festival-goers to prove their identity.

High rates of misidentifications by automated facial recognition cameras affect everyone, but are particularly disturbing in light of research showing that many facial recognition algorithms disproportionately misidentify black people and women. In the context of law enforcement, biased facial recognition algorithms risk leading to disproportionate interference with the groups concerned – whether through police stops and requests to show proof of identity, or through the police's storage of 'matched' biometric photos.

A recent study conducted by the Massachusetts Institute of Technology into the commercial use of artificial intelligence systems found that the error rate of facial recognition software was 43 times higher for dark-skinned women than it was for light-skinned men.[16]

In fact, numerous studies have similarly found that facial recognition algorithms – including the FBI's - disproportionately misidentify black faces. [17] The causes of this algorithmic discrimination may vary, but are likely due to the fact that the datasets on which the algorithms are trained contain mostly white and male faces, as well as the fact that cameras are not configured to identify darker skin tones.[18]

However, the commercial facial recognition software used by South Wales Police and the Metropolitan Police, NEC's NeoFace Watch, has not been tested for demographic accuracy biases. We, and fellow rights and race equality groups, have urged the forces to seek such testing.

The Scottish Government's independent review of biometrics highlighted the worrying trend for the outsourcing of such advanced technology to the private sector, without properly evaluating the technology and testing for accuracy biases:

> *"[B]iometric image capture technologies are increasingly sourced from the private sector. This results in a gap in scope for independent evaluation of the effectiveness of technologies whose biometric identification algorithms are protected by issues of commercial confidentiality"*[19]

We have been extremely disappointed to encounter resistance from the police in England and Wales to the idea that such testing is important or necessary.

In addition, Metropolitan Police officers told us they would not record ethnicity figures for the number of individuals identified, whether correctly or incorrectly, by the facial recognition system as they viewed the data as unnecessary and unimportant. Therefore, any demographic disproportionately in this this hi-tech policing will remain unaccountable and hidden from public view.

Many organisations are concerned by this technology and the risk of it carrying invisible, unaccountable demographic biases. Before the Metropolitan Police used automated facial recognition for the second time at Notting Hill Carnival in 2017, Big Brother Watch, Police Action Lawyers Group, the Race Equality Foundation, and 10 other rights and race equality groups signed a joint letter to the force raising our concerns and calling for a halt to the deployment.[20] Our concerns were not addressed.

Disproportionate misidentifications risk increasing the over-policing of ethnic minorities on the premise of technological 'objectivity'. This issue will be further compounded if police disproportionately deploy automated facial recognition in areas with high BME populations, such as the Metropolitan Police's repeated targeting of Notting Hill Carnival using the British African Caribbean community as guinea pigs for this authoritarian new technology.

Stop, Search and Facial Recognition

A contribution from Samir Jeraj, Policy and Practice Officer at the Race Equality Foundation:

A few Christmases ago, I was walking through the main street of the town I grew up in. Across the street, a young Asian man was stopped by the Police. I looked for a while, realised it was going to take some time and went over to see what was happening. I took out my phone to record what was happening. Short version: the young man matched the description of a guy who had shoplifted from a supermarket. He had no ID on him, so the Police stopped him while they confirmed his identity.

They handcuffed him behind his back and kept him standing out on the high street, which was totally unnecessary – he was annoyed about being stopped but no more so than anyone else would be in that situation. After a few minutes it became clear he wasn't the Asian man they were looking for and released him. During the incident a Police officer (wrongfully) claimed they could seize my phone as evidence, despite my being a journalist and such a seizure being subject to a warrant. I tried to find the young man later on Facebook to send him the video, but couldn't.

What this story should tell you is the power of misidentification. In this case, it led to a young man being handcuffed, on a busy high street, and may have permanently damaged his trust in the Police (it definitely left me more wary). 51% of the UK-born Black and minority ethnic population believe 'the criminal justice system discriminates against particular groups',[21] compared to 35% of the UK-born white population.

'Profiling' of black and minority ethnic communities has a long history in the UK. Ranging from continued disproportionate use of stop and search powers,[22] through evidence of prejudice and bias in policing culture[23], and intensive surveillance[24] of black and minority ethnic communities.

The capacity for facial recognition to be used on a large group fits into this pattern of profiling. It also makes the chance of this type of misidentification, and the subsequent impact on people, all the more likely. Where facial recognition technology has been used in the United States, using a much larger database of images collected through driving licenses, it has been found to be racially biased. In one study, where the technology was able to make a match it was wrong 12% of the time for black and minority ethnic men, and 35% of the time for black and minority ethnic women.[25]

The racial issues and discrimination in policing are so well known that in his recent review of Criminal Justice,[26] David Lammy MP said it was not even worth including. The clear message from what the Lammy Review did look at, namely what happens after arrest, is that black and minority ethnic people are subject to inequalities at all stages of criminal justice.

In some ways, it was a relatively mild outcome for the young man. Had he been a bit more annoyed, or been perceived to have been, he may have ended up restrained, harmed, arrested and charged with a public order offence. If he had been, he would have been 16% more likely to be remanded in custody, and if he were convicted he would be almost five times more likely to be housed in high security.[27]

However, there is a much broader issue of consent and transparency. In the UK, deployment of facial recognition has been shrouded in opaqueness if not outright secrecy. Rather than allowing a full and open examination of the technology, the algorithms[28] and the approach to policing, facial recognition has been used almost as a propaganda tool. The announced use at Notting Hill Carnival[29] is one

example of this, where it was likely part of the usual strategy of trying to persuade people not to come[30] – a legacy of the history of poor policing of Carnival.

The risk is that policing becomes reactive and based on a philosophy of crime suppression, as it has become in the United States. Something that would inevitably lead to greater use of force,[31] disproportionately towards black and minority ethnic people, and terrible consequences for those wrongly identified.

We are deeply concerned about the impact of automated facial recognition on individuals' rights to a private life and freedom of expression, and the risk of discriminatory impact.

Facial recognition and the unlawful retention of custody images in the UK

Section 64A of the Police and Criminal Evidence Act 1984 (PACE) provides police with the power to take facial photographs (custody images) of anyone who is detained following arrest. Forces can upload custody images from their local IT systems onto the Police National Database ('PND'), which has been in place since 2010.

The PND was upgraded to include a facial recognition search function on 28th March 2014. This upgrade happened without parliamentary or public scrutiny. However, a large portion of people who are arrested and have a custody image taken are never charged or convicted of any crime.

The PND currently holds 19 million custody images[32] of which, according to the Biometrics Commissioner, hundreds of thousands[33] relate to innocent people – most of whom are not even aware that biometric technology is used on their images. However, a staggering 12.5 million photographs on the PND are already biometrically searchable with facial recognition.[34]

With more and more biometric images being fed into the database – subsets of which are used with real-time facial recognition cameras - innocent people are increasingly at risk of being wrongfully stopped or even arrested.

It is not known how many images on the Police National Database are of innocent people – our investigation reveals that neither the Home Office nor the police can keep count. The police seem to have lost control over managing who should be on their databases and who should be removed.

Based on Freedom of Information requests sent by Big Brother Watch to 45 UK police forces, not a single force that responded to the request was able to determine how many of their custody images were of innocent people.

In fact, there is no process in place that allows police forces to easily find and remove those images from their databases. The forces stated that they would have to manually review each file and cross reference between local and national databases to establish who had been convicted and who was innocent. Forces estimated the time needed to review each file between 3 to 10 minutes.

For example, Kent Police estimated the following:

> *"As an example in 2015 there were 29,056 arrests. [...]Based on previous experience of researching local and national databases it is likely to take in the region of 5 minutes to determine whether a person associated to a custody record has an image stored by Kent Police and has been convicted of an offence. Therefore using 2015 as an example, 29,056 x 5 minutes = 145,280 minutes (2,421.33 hours)."*

That means it would take one member of staff at Kent Police, working full-time and allowing only five minutes per custody image review, over one year to separate just one year's worth of arrests into convicts and innocent people whose images should not be retained.

In March 2018, Baroness Williams repeated the Home Office line that deleting unconvicted people's custody images would be too expensive, claiming that it would have to be done "*manually*", would have "*significant costs*", and would apparently therefore "*be difficult to justify*".[35]

Clearly, the administrative burden caused by police data retention systems that are not fit for purpose and that are predicated on an unworkable 'collect it all' approach is significant.

The Home Office claims that they "*expect the new platform being delivered by the National Law Enforcement Data Programme to resolve this in the medium term by enabling a considerably more flexible approach to automatic deletion*".[36] It is troubling that this is not a firm commitment - a vague 'expectation' about capabilities 'in the medium term' is unacceptable. In any event, an interim solution must be provided immediately.

The Government should provide funding for administrative staff in each police force to deal with this problem until the new law enforcement database is in place, to protect individuals' data protection rights and Article 8 right to privacy, and to ensure that forces are complying with their legal obligations.

The alternative is unacceptable – that the state accrues an ever-increasing database of biometric photographs of millions of innocent people in a flagrant breach of the law.

In *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012][37] the High Court ruled that the indefinite retention of innocent people's custody images was unlawful. However, neither the Home Office nor police forces have taken the necessary steps to put these policies into place. The police continue to indiscriminately store custody images.

In February 2017, following a review, the Government gave unconvicted individuals the option to write a letter to the relevant police force to request deletion of their image from the custody image database – although it did nothing to publicise this avenue to the public or those affected. This obstructive policy shirks responsibility from the Home Office, which clearly needs to automatically delete the thousands of images stored of innocent people.

The new policy was exposed as a failure by a Press Association investigation in February 2018 which found that only 67 applications for deletion had been made, of which only 34 were successful.[38] Norman Lamb MP, Chair of the Science and Technology Committee, publicly commented on his concerns that the Home Office's retention and deletion-on-request policies are likely to be unlawful.[39]

'Costs' are not an acceptable reason for the British Government not to comply with the law – and costs are hardly a convincing reason, given that the Home Office has awarded £2.6million to South Wales Police to deploy automated facial recognition matching people's faces in real-time against those same custody images. In fact, if the Home Office were to fund all 45 police forces in the UK £35,000 to hire an administrator to manually review custody images, the cost for one year would be £1.5million.

In his 2016/17 Annual Report, the Surveillance Camera Commissioner commented:

> *"[The Custody Images Review 2017] directly relates to the use of automatic facial recognition systems because the police will seek to utilise this database to build the systems for cross checking live feeds from surveillance cameras against this database."*[40]

We are now witnessing police forces do exactly that - using subsets of the custody image database to match against live CCTV feeds with automated facial recognition software.

In his 2016 Annual Report, the Biometrics Commissioner commented:

> *"The use of facial images by the police has gone far beyond using them for custody purposes (...) (U)nlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge and facial images of about 90% of the adult population already exist in passports or driving licences."* [41]

Clearly, the potential for the growth of a gargantuan facial recognition system is a real risk, and arguably would be the natural destination for this technology, if we so uncritically accept its use now.

We call on the Home Office to automatically remove the thousands of images of unconvicted individuals from the Police National Database.

Automated facial recognition and law enforcement in the UK

No other democratic country in the West has implemented automated facial recognition surveillance cameras in law enforcement as rapidly and recklessly as the UK.

Thus far, three forces - Leicestershire Police, Metropolitan Police and South Wales Police – have deployed or continue to deploy automated facial recognition with CCTV cameras in public spaces.

Leicestershire Police

Leicestershire Police was the first force in the UK to deploy live facial recognition software. The force used automated facial recognition at Download Festival in June 2015, where 90,000 festival goers were checked against a Europol database. This was the first time automated facial recognition had been used at an outdoor event in the UK. Leicestershire Police stated that they deleted captured images after the event.[42]

Metropolitan Police

New statistics

The staggering ineffectiveness of the technology has been revealed by a series of Freedom of Information requests we made to the Metropolitan Police. The statistics we have received show that their use of automated facial recognition has resulted in 'matches' with less than 2% accuracy, with over 98% of matches wrongly identifying innocent members of the public.

The force reported it has had a total of 102 false-positive 'matches' in the course of trialling automated facial recognition – that is, 102 innocent people incorrectly identified by the system, the majority of whom will be attendees of Notting Hill Carnival.

Our research reveals that, unbeknown to these people, a biometric photo was taken of them and stored by the police for 30 days.

The force has only correctly identified 2 people using the technology – neither of which was a wanted criminal. One of those people matched was

the individual at Notting Hill Carnival 2017 incorrectly included on the watch list; the other was on a mental health-related watch list at Remembrance Sunday 2017.

The force has made 0 arrests using the technology.

Notting Hill Carnival 2016 and 2017

The Metropolitan Police first used automated facial recognition at Notting Hill Carnival 2016. The force claimed that scanning the faces of Carnival goers using facial recognition would help to identify wanted offenders, people on bail conditions not to attend, and "*known criminals*".[43] However, during the two day event, police reported that *"no individuals were identified by the equipment."* [44]

The following year, the Metropolitan Police ran another 'trial' of facial recognition at Notting Hill Carnival, this time facing strong opposition from rights and race equality organisations, as well as the wider public. Being the largest African-Caribbean event in the UK, strong criticism was voiced against racial profiling and the over-policing of Black communities.[45] Our FOI work reveals that 528 people were on the watch list, including not only people wanted for arrest but "known criminals". Therefore, we are concerned that real-time facial recognition is being used for intelligence purposes and risks perpetually stigmatising people who may be trying to move on from their criminal histories.

Big Brother Watch, Liberty, the Race Equality Foundation and ten other rights and race equality groups wrote to the Commissioner of the Metropolitan Police ahead of the event to voice our opposition. We did not receive a reply before the event. However, after remonstrating, Big Brother Watch, Liberty and StopWatch were permitted to observe the facial recognition cameras operating for a short period at Notting Hill Carnival 2017. In our 5- 10 minute observation of the technology in action, we witnessed two false-positive matches. Both times, unsuspecting innocent women were matched with men on the database - confirming the astounding inaccuracy of this technology.

The police informed us that there had been around 35 false-positive matches just on that one day. The police reported that they had staged interventions with "*around five*" Carnival-goers, whereby innocent people incorrectly matched by the system were apprehended and asked to prove their identity and thus their innocence. Over the whole weekend there was only one positive match – however, the person stopped was no longer wanted for arrest, as the police's data compiled for the event was outdated.

In a letter to the Science and Technology Committee on 28 March 2018, Baroness Williams, Minister for the Home Office, stated that the watch list used at Notting Hill Carnival included "*people involved in... sexual assault*".[46]

We reject this justification and question why the police are not carrying out their statutory functions by using their resources to actively find individuals wanted for arrest as soon as possible, especially for offences as serious as sexual assault. We are concerned that police cuts may be a contributing factor as, in response to one of our FOI requests, the force told us they want to "*explore technical solutions to locating and arresting wanted offenders using minimal resources*".[47] The idea that police should use hi-tech, intrusive surveillance and biometric tracking as a passive catch net for people wanted for arrest is an absurd and dangerous technophilic fantasy that would rapidly securitise free public spaces.

Remembrance Sunday 2017

On Remembrance Day 2017, the Metropolitan Police used automated facial recognition to effectively police mental health, scanning the faces of thousands of people paying their respects to match against a database of 42 'fixated' individuals[48] - people who are known to frequently contact public figures.

So-called 'fixated individuals' are identified by the 'Fixated Threat Assessment Centre' (FTAC), a joint unit run by the Metropolitan Police, Home Office and Department of Health.[49] These are individuals who typically suffer from serious mental health issues. They are not criminals, and none of the individuals on the watch list was wanted for arrest. Our FOI investigation reveals that their photos were obtained "*usually outside a protected site or during a previous event*".[50]

In a letter to the Science and Technology Committee on 28 March 2018, Baroness Williams, Minister for the Home Office, attempted to defend the legitimacy of police use of automated facial recognition, stating that it is only used to compare people's faces against "*watch lists*" populated "*with images of individuals forbidden from attending the events*" or "*individuals wanted by police*".[51] However, this evidently was not the case at Remembrance Sunday where the watch list was comprised of individuals who were not forbidden from attending the event nor wanted by the police.

This non-criminal application of facial recognition technology resulted in a so-called 'fixated individual' being identified and subsequently dealt with by police. We have been told different versions of events by officers, varying from the individual being subsequently ejected from the event, to the individual being effectively accompanied by police during the service.

In our engagement with the police after the deployment, we were told that they had not consulted mental health groups or sought appropriate advice from experts. Critically, they had not considered the impact that this intrusive biometric surveillance and intervention by the police could have on vulnerable individuals' mental health.

We view this deployment as a chilling example of function creep and the dangerous effect automated facial recognition can have on fundamental rights – particularly those of the most marginalised in society.

South Wales Police

South Wales Police has taken a national lead in the roll-out of automated facial recognition.

New statistics

Our research reveals that the force was awarded a total of £2.6m by the Government to carry out automated facial recognition - £1.2m in 2016/2017 and £0.8m for 2017/18 by the Home Office,[52] as well as £0.6m from Home Office Biometrics. South Wales has additionally contributed £100,000.[53]

South Wales Police deployed "AFR Locate" for the first time on 29 May 2017, during the UEFA Champions League final. The force confirmed that in less than a year they had utilised the system 18 times. South Wales' deployment of automated facial recognition is typically in relation to petty criminals with a history of low level offences such as pick-pocketing.[54]

Neither South Wales Police nor the Metropolitan Police is using automated facial recognition with public surveillance cameras in relation to national security.

Events automated facial recognition deployed at	Dates
UEFA Champions League Final Week	Week commencing 29/05/2017
Elvis Festival	23/09/2017 - 24/09/2017
Operation Fulcrum (Day of Action)	19/10/2017
Anthony Joshua v Kubrat Pulev (Boxing)	28/10/2017
Wales v Australia Rugby	11/11/2017
Wales v Georgia Rugby	18/11/2017
Wales v New Zealand Rugby	25/11/2017
Wales v South Africa Rugby	02/12/2017
Kasabian Concert (Motorpoint Arena, Cardiff)	04/12/2017
Liam Gallagher Concert (Motorpoint Arena, Cardiff)	13/12/2017
Operation Fulcrum (Day of Action)	22/12/2017
Operation Malecite (Festive Deployment)	23/12/2017
Royal Visit (Prince Harry)	18/01/2018
Wales v Scotland Rugby	03/02/2018
Wales v Italy Rugby	11/03/2018
Wales v France Rugby (Cardiff City Centre)	17/03/2018
Arms Fair Demonstration (Motorpoint Arena, Cardiff)	27/03/2018
Anthony Joshua v Joseph Parker (Boxing)	31/03/2018

Responses to our Freedom of Information requests reveal that South Wales Police had a total of 2,685 'matches' using automated facial recognition between 29th May 2017 and 11th March 2018 (i.e. excluding the most recent three deployments for which, at the time of writing, we do not have statistics). However, less than 9% (234) of these alerts were accurate. A staggering 91% of 'matches' - 2,451 - incorrectly identified innocent members of the public.

Our investigation also reveals that South Wales Police is indiscriminately storing captured photos of both true-positive and false-positive matches for 12 months. This unprecedented approach means that biometric photos captured of at least 2,451 innocent people who have wrongfully been 'matched' by facial recognition software remain in the hands of the police, entirely without their knowledge.

Whilst the force claimed 234 alerts were accurate matches, they reported only 110 interventions and 15 arrests - amounting to just 0.005% of 'matches'. When asked to explain this discrepancy, the project lead explained that "alerts may have been for intelligence only". We are incredibly disturbed by the use of biometric tracking in day-to-day policing for 'intelligence' purposes.

Furthermore, at least twice as many innocent people than those arrested have been significantly affected, as police have staged interventions with 31 innocent members of the public. 31 people incorrectly identified by the system were asked to prove their identity and thus their innocence.

Pervasive deployments

South Wales Police's introduction of automated facial recognition into day to day policing is highly concerning. Several of the force's deployments around the Christmas period targeted retail centres rather than specific events – and city centres appear to be targeted around event surveillance too. On 17th March 2018, in conjunction with a deployment at a Six Nations rugby match, South Wales Police's automated facial recognition project lead Scott Lloyd announced the deployment of the technology in Cardiff's city centre on Twitter. These routine deployments demonstrate that citizens are being increasingly subjected to identity checks while going about their daily lives.

Automated facial recognition at a peaceful protest

Big Brother Watch was alarmed to discover that South Wales Police used automated facial recognition to surveil a peaceful demonstration outside an arms fair, the Defence Procurement Research Technology Exhibition (DPRTE), on 27th March 2018.[55] Free speech, protests and demonstrations are vital democratic forms of expression. No citizen living in a democratic nation should expect to be subjected to biometric identity checks and recorded by state CCTV when exercising their fundamental right to demonstrate.

Innocent demonstrators incorrectly identified by the cameras will have no idea that their biometric photos are now stored on a police database for a year.

The biometric surveillance of this arms fair demonstration is a prime example of how the opportunistic deployment of automated facial recognition, practised without any legal basis, can be abused to target dissidents or other 'problematic' groups.

Given South Wales Police's prolific use of automated facial recognition it is hard to believe that they are still in a 'pilot' stage – on the contrary, automated facial recognition appears to already be firmly incorporated into their general policing practices.

Future uses

Facial recognition and integrated CCTV networks

In March 2018, City of London Police proposed upgrading the so-called 'ring of steel' ANPR and CCTV network around the city with facial recognition.[56] London is already the most surveilled city in the world, beaten only by Beijing. An additional facial recognition ring of steel would make the city an oppressively securitised zone, with its residents and millions of visitors among the most surveilled people in the world.

Similarly, West Yorkshire Police applied for Home Office funding in August 2017 to develop facial recognition for use on public space CCTV and Metro transport CCTV in conjunction with Safer Leeds, Bradford Metropolitan District Council (MDC), Calderdale MDC, Kirklees MDC, Wakefield MDC, Community Safety Partnership (CSP), Metro and Five West.[57] A report said:

> *"A bid was put into the Home Office Innovation fund by West Yorkshire to look at co-ordinated public service CCTV capacity across West Yorkshire offering inter-operability between the five local authorities and Metro with the further potential for integrated technology including facial recognition aimed at protecting vulnerable missing persons."*[58]

Post video analysis

European IT company SCC has collaborated with video intelligence company SeeQuestor to provide post analytical video services to over 40 UK Police Forces:

> *"The Video Analytics (VA) solution will provide UK forces with advanced post-event video analytics allowing them to view and analyse large amounts of Mobile, CCTV and Body Worn Video formats to support the prosecution process. This service, which is part of the developing portfolio of SCC Public Safety Solutions, is underpinned by the pioneering SeeQuestor platform. This will provide video ingestion, conversion, case management and an analytics capability including face, body and attribute detection, and subject re-identification."*[59] *(January 2018)*

The video analytics 'solution' already offers person detection and tracking, and given that it already provides face detection, is technically one step away from providing biometric facial recognition to recorded video analysis. Police forces can already take stills from CCTV feeds and use facial recognition to search for a match across the PND.

Mobile facial recognition

The current capabilities of facial recognition are fast developing, making it easier to integrate the biometric tracking software across multiple devices. Japanese company NEC, which provides facial recognition software to UK police forces, acquired Northgate Public Services (NPS) for £475million in January 2018. NPS supplies UK police forces with CONNECT.

The CONNECT platform provides an integrated police information system across desktop to mobile applications in real-time, including a broad range of data, information and intelligence.[60] During the acquisition, it was reported that:

> *"One of the key advantages of the acquisition, the two parties claim, will be the opportunity for NPS to integrate NEC's facial-recognition and other biometric technologies into its software products."*[61]

West Yorkshire Police, which began deploying controversial mobile fingerprint scanners linked to both criminal and immigration databases in February 2018, has vowed that mobile facial recognition will be in deployment "*within 12 months*".

Even local authorities are seeking to utilise this authoritarian technology. We were concerned to learn that Milnbank Housing Association issued Police Scotland with hand held devices in March 2018 equipped with "*facial recognition and number plate recognition*" which enables the user to "*identify persons of interest and track their movements*."[62] It is intended that the force will use this new capability to police the Haghill housing estate in Glasgow.

Resistance to facial recognition around the world

Germany - has the train already left the station?

Great controversy was caused when Germany's Federal Minister of the Interior, Thomas de Maizière, commissioned a pilot of live facial recognition technology at Berlin's Südkreuz railway station in August 2017. Equipped with three facial recognition enabled surveillance cameras, the pilot was supposed to run for six months and invited 250 volunteers to participate in the trial.

The project prided itself on transparency and taking the privacy of non-participants into account by putting up signage and restricting the use of the cameras to a specific area. However, critics point out that volunteers were incentivised to subject themselves to the biometric surveillance with the promise of prizes like 'smart' watches for the participant who got captured most by the system. Nevertheless, any member of the public who entered the surveilled areas would still involuntarily have their faces scanned if not identified.

The Minister recently announced that the trial would be prolonged for six further months,[63] which means that up to 100,000 people will be scanned on a daily basis.[64] It is questionable why German authorities decided to extend the pilot. Even under the controlled environment of the trial, the system correctly matched volunteer images only 70-85% of the time[65] – demonstrating that the technology is unreliable and inaccurate.

The pilot at Berlin Südkreuz was met with significant public protest in Germany, particularly given their new law allowing police forces and other authorities to access citizens' biometric passport and ID images. The German Bar Association pointed out that the use of facial recognition violates citizens' fundamental rights.[66] The President of the Association emphasised that: "*This interaction between technical and legal innovations poses an unprecedented threat to the protection of civil liberties*".[67]

Russia - 160,000 cameras to follow citizens around the clock

In September 2017, Moscow's local government announced the formal deployment of live facial recognition technology, acquired from start-up NTech Lab, on the city's 160,000 camera strong CCTV network.[68] The city's Department of Information Technologies claims the surveillance system covers 95% of apartment building entrances in Moscow.[69]

Although facial recognition is only active on a few cameras at a time, it can quickly be changed to target areas of interest. Authorities claim that they own the world's largest CCTV network and needed artificial intelligence to sift through masses of footage accumulated. Unlike in the UK, Germany or the US, the use of this extended surveillance machine is authorised by national law.[70]

China - the new frontline laboratory for surveillance

China's prolific use of surveillance technology has been widely criticised by observers and particularly human rights advocates. China's introduction of live facial recognition technology across the country has invited particular scrutiny.

Combined with a pervasive video surveillance network, live facial recognition technology enables authorities to track a citizen seamlessly through large parts of Chinese cities. Individuals and vehicles can be recognised by the system whereupon law enforcement is alerted to their movements.[71]

Currently, there are 170 million CCTV cameras across China.[72] In March 2018, as part of the nationwide monitoring program 'Skynet', cameras in 16 parts of the country were upgraded with automated facial recognition software, enabling the identification of millions of citizens within a second by the cameras.[73]

Chinese developers have even successfully integrated facial recognition into 'smart' sunglasses, enabling the police to patrol Beijing's outskirts and check travellers' identities independently from surveillance cameras.[74] With the help of facial recognition and AI, jaywalkers are now publicly named and fined via text messages.[75]

Official statements claim that the use of the technology is limited to catching criminals. However, ethnic minorities and dissidents are frequently being targeted.

For example, the North West province Xinjiang has cynically been called a 'Frontline Laboratory for Surveillance'.[76] At the beginning of 2018, a live

facial recognition system was tested that alerted officials when a target moved more than 300m away from their home or workplace. Authorities stated that these measures were trialled to target terrorists and extremists hiding in the area. However, the targeting of the province's Muslim Uighur minority is striking,[77] as they can be arrested for suspected political disloyalty or simply expressing their religious and cultural identity. In combination with other biometric and behavioural-predictive technologies, facial recognition assaults the privacy rights of innocent people and enables the indiscriminate targeting of Uighurs.[78]

China's extensive deployment of facial recognition should not be dismissed as an exceptional or distant risk to the West. It is proof that the technological capability to watch citizens 24/7 and erode their personal freedoms already exist and could easily be applied anywhere. This example should be a warning to any free democracy to take a critical and cautious approach to surveillance technologies that fundamentally threaten citizens' civil liberties and privacy.

The United States - intrusive facial recognition in the land of the free

In contrast to the UK, stadiums and other outdoor spaces are often privately owned in the United States. Therefore, the use of automated facial recognition at large scale events often lies in the remit of commercial actors. For example, in March 2018 it was revealed that operators of Madison Square Garden used the technology on visitors without their knowledge.[79]

US police departments have also started to implement the technology, sparking great controversy around their actions. A report from the Center on Privacy and Technology at Georgetown Law found that "*at least five major police departments—including agencies in Chicago, Dallas, and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed an interest in buying it.*"[80]

Like in the UK, the use of facial recognition technology by law enforcement in the US is unregulated and without a legal basis - only five states have laws that vaguely address the issue.[81] As is the case in any democratic country, the use of facial recognition heavily collides with the rights of US citizens - particularly the First and Fourth Amendments.

Contribution from

Jay Stanley, senior policy analyst with the ACLU Speech, Privacy, and Technology Project

The use of Face Recognition in the United States appears to be on the verge of taking off. Our customs agency is ramping up its use in tracking those entering and leaving the United States, and our airline security agency is contemplating its use for tracking passengers within U.S. airports. Local police and the FBI have used driver's license databases to enroll half of Americans in law enforcement face-photo databases.

Police departments in major cities are also exploring the use of real-time face recognition on live surveillance camera video. Companies are selling, and police appear to be contemplating adopting, body cameras that include such real-time face recognition.

Because of a lack of transparency we don't know exactly how widely or often the technology is being used by law enforcement. Such use hasn't been subject to proper democratic debate, systematic oversight, or controls or testing to measure for accuracy or bias. Law enforcement use also inevitably reflects the racial bias that pervades the U.S. criminal justice system. In addition to the fact that the technology can be less accurate when trying to identify people of colour, Black people are overrepresented in face recognition databases.

American companies, meanwhile, unconstrained by a comprehensive data privacy law, are operating in a Wild West with virtually no legal restraints on their use of the technology. Facebook, which holds the largest collection of facial photos in the world, does not give its users the option to not make those photos public, making them susceptible to scraping by such companies.

Face recognition is a powerful surveillance technology that has the potential to change the nature of public life in the United States. We are a democracy, so decisions about how we want to allow such a technology to be used should be made through the political process, but that isn't happening.

If we as a society decide to allow for the untrammelled use of face recognition, we are likely to end up with an infrastructure for surveillance and tracking that is far more powerful and systematic than anything that can be done with surveillance cameras alone. This threatens to have an enormous chilling effect on public life, to shift power away from individuals and toward already powerful institutions such as government agencies and corporations, and greatly intensify

the risks of abuse. That risks draining our First and Fourth Amendment rights to free expression and privacy of substance and meaning, and makes it imperative that we act soon to put in place common sense restrictions on how this technology is deployed in American life.

Contribution from

Clare Garvie, Associate, at Georgetown Law Center on Privacy and Technology, co-author of "The Perpetual Line-up - Unregulated Police Face Recognition in America"

Face recognition use by U.S. law enforcement is far more pervasive, and advanced, than most people assume. By now most photo databases maintained by state and federal agencies—visas, passports, driver's licenses, mugshots—are face recognition-enabled. And irrespective of the original purpose for which the photos were collected, these databases are increasingly accessible to police.

Face recognition surveillance — identifying people in real-time from live video feeds — risks being an imminent reality for many Americans. Are we comfortable with a society where face recognition allows police to identify anyone with a driver's license, without suspicion or consent? Are we comfortable with a society where the government can find anyone, at any time, by continuously scanning the faces of people on the sidewalk? Face recognition fundamentally changes the nature of privacy in public spaces. As government agencies themselves have cautioned, face recognition surveillance 'has the potential to make people feel extremely uncomfortable, cause people to alter their behaviour, and lead to self-censorship and inhibition,' chilling the exercise of the rights protected under the First Amendment and calling into question the scope of protections offered by the Fourth Amendment.

U.S. legislatures and the courts have begun limiting other advanced police tracking technologies — license plate readers, geolocation tracking devices, drones. To date, there are no comprehensive state or federal laws governing how police can — or more importantly cannot — use face recognition. As a consequence, it is up to agencies to police themselves; unsurprisingly, many have failed to implement even the most basic accountability measures. It is past time for American legislators to consider the implications of this powerful technology, and to reign in its use.

Contribution from

Jennifer Lynch, Senior Staff Attorney at the Electronic Frontier Foundation (EFF), author of a white paper on police use of facial recognition in the United States

Face recognition is poised to become one of the most pervasive surveillance technologies of the 21st Century. Today, police officers use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face identification; and law enforcement agencies have access to databases of hundreds of millions of face images of law-abiding citizens. In some countries, police officers are already using face recognition with body-worn cameras, and in the near future, we'll see face recognition used to identify people in the dark and even to construct an image of a person's face from a small sample of their DNA.

However, the adoption of technologies like these is occurring without meaningful oversight, without proper accuracy testing, and without the enactment of legal protections to prevent misuse. If we move forward on this path, these systems will mistakenly identify innocent people as criminals or terrorists and will be used by unscrupulous governments to silence unwelcome voices.

We must act now to curb the use of face recognition by governments and law enforcement. Without public action, we will see the development of unproven, inaccurate systems that will disproportionately impact people of colour and impinge on the human rights of all people.

Conclusion

Big Brother Watch believes in a world where citizens are free from suspicionless surveillance, discrimination, oppression and unfair intrusion.

Surveillance technologies are developing at a breakneck speed that is hard to follow. Technological developments prompt us to ask critical questions about the future of civil liberties in the UK – do we want to live in a world where citizens are continuously watched, intrusively surveilled, and biometrically tracked? What are the risks to public freedoms, to our democratic norms, to our fundamental rights?

The lawless growth of facial recognition in UK policing affects all British citizens, but as exposed in this report, it worst affects the most marginalised in our society.

This authoritarian surveillance practice has been levelled against minorities, peaceful demonstrators, and mentally unwell citizens without any guiding law, oversight, or formal scrutiny.

We are deeply concerned that the securitisation of public spaces using biometrically identifying facial recognition unacceptably subjects law abiding citizens to hidden identity checks, eroding our fundamental rights to privacy and free expression.

Action must be taken, now.

- We call on UK public authorities to immediately stop using automated facial recognition software with surveillance cameras.
- We are deeply concerned about the impact of automated facial recognition on individuals' rights to a private life and freedom of expression, and the risk of discriminatory impact.
- We call on the Home Office to automatically remove the thousands of images of unconvicted individuals from the Police National Database.

Endnotes

[1] Garvie, Clare; Bedoya, Alvaro M.; Frankle, Jonathan; Georgetown Law Center on Privacy and Technology: The Pertual Line-Up – Unregulated Police Face Recognition in America, p.9, 18 October 2016. Available from https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

[2] https://www.flickr.com/photos/samchurchill/ -CC BY 2.0

[3] Lynch, Jennifer; *Electronic Frontier Foundation*: Face Off – Law Enforcement Use of Face Recognition Technology, p.2, February 2018 [viewed on 12/02/2018]. Available from https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf

[4] NEC website, *Putting More Than Just a Name to a Face*. Available from https://www.nec-enterprise.com/products/NeoFace-15

[5] Written parliamentary question answered by Mr Nick Hurd MP on 12 September 2017.

[6] *A National Surveillance Camera Strategy for England and Wales* – Surveillance Camera Commissioner, March 2017, para. 35, p.12

[7] Review of the impact and operation of the Surveillance Camera Code of Practice –Surveillance Camera Commissioner, Feb 2016, p.15

[8] Letter from Baroness Williams, Minister for the Home Office, to the Chair of the Science and Technology Committee, 30 November 2017 http://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/171130-BWT-to-Chair-biometric-strategy.pdf

[9] Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

[10] South Wales Police and Crime Commissioner, 'Medium Term Financial Strategy 2017-2021', 28 December 2016 https://pcclivewww.blob.core.windows.net/wordpress-uploads/2016-12-28-Final-Medium-Term-Financial-Strategy.pdf p.49

[11] Report of the Independent Advisory Group on the Use of Biometric Data in Scotland, 21 March 2018, http://www.gov.scot/Resource/0053/00533063.pdf

[12] Biometric Commissioner, *Annual Report 2016*, September 2017, para. 305

[13] The Lord Bishop of St Albans in question for short debate, Security and Policing: Facial Recognition Technology in the House of Lords, 1 March 2018, Hansard, vol. 789, col. 801

[14] South Wales Police, *Introduction of Facial Recognition into South Wales Police*, 2017 (https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/)

[15] Daily Record, *Scottish football fans unite against SPFL's bid to bring in facial recognition cameras: 'Plan will drive punters away*, 21 January 2016 (https://www.dailyrecord.co.uk/sport/football/football-news/scottish-football-fans-unite-against-7217114)

[16] Buolamwini, Joy; Gebru, Timmit: Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research 81:1, p.1-15, 2018. Available from http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, p.1.
The study analysed the software made by Microsoft, IBM and Face++, which provides its software to the Chinese government.

[17] Klare, Brendan F.; Burge, Mark J.; Klontz, Joshua C.; Vorder Bruegge, Richard W., Jain, Anil K.: Face Recognition Performance: Role of Demographic Information. In: IEEE Transactions on Information Forensics and Secuirty, p.3. Available from http://openbiometrics.org/publications/klare2012demographics.pdf

[18] Buolamwini, Joy; Gebru, Timmit: Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research 81:1, p.1-15, 2018. Available from http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, p.11

[19] Report of the Independent Advisory Group on the Use of Biometric Data in Scotland, 21 March 2018, para 2.5 http://www.gov.scot/Resource/0053/00533063.pdf

[20] Letter from 13 NGOs to the Commissioner of the Metropolitan Police, 16 August 2017. Available from https://www.libertyhumanrights.org.uk/sites/default/files/Joint%20letter%20to%20Met%20-%20AFR%20FINAL.pdf

[21] Lammy Review: emerging findings published, 16 November 2016, Available from https://www.gov.uk/government/news/lammy-review-emerging-findings-published

[22] Dodd, Vikram, *The Guardian*: Stop and search eight times more likely to target black people, 26 October 2017. Available from https://www.theguardian.com/law/2017/oct/26/stop-and-search-eight-times-more-likely-to-target-black-people

[23] *BBC News Online*: Black police leader says some forces 'still institutionally racist', 17 January 2018. Available from http://www.bbc.co.uk/news/uk-england-42702432

[24] Dwyer, Danielle; Johnson, Wesley, *The Independent*: Police apologise over CCTV in Muslim areas, 30 September 2010. Available from https://www.independent.co.uk/news/uk/crime/police-apologise-over-cctv-in-muslim-areas-2094167.html

[25] Lohr, Steve, *The New York Times*: Facial Recognition Is Accurate, if You're a White Guy, 9 February 2018. Available from https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[26] Lammy review: final report, 8 September 2017 https://www.gov.uk/government/publications/lammy-review-final-report

[27] Lammy Review: emerging findings published, 16 November 2016, Available from https://www.gov.uk/government/news/lammy-review-emerging-findings-published

[28] Breland, Ali; *The Guardian*: How white engineers built racist code – and why it's dangerous for black people, 4 December 2017 https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police

[29] Dodd, Vikram, *The Guardian*: Met police to use facial recognition software at Notting Hill carnival, 5 august 2017. Available from https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival

[30] Alemoru, Kemi; Dazed Digital: A history of The Met Police's hatred of Carnival, 23 August 2017. Available from http://www.dazeddigital.com/life-culture/article/37150/1/the-police-notting-hill-carnival

[31] Pilkington, Ed, The Guardian: US police departments are increasingly militarised, finds report, 24 June 2014. Available from https://www.theguardian.com/law/2014/jun/24/military-us-police-swat-teams-raids-aclu

[32] *Press Association:* 'Custody image' deletion request figures revealed, 12 February 2018 [viewed on 12/02/2018]. Available from http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.html

[33] *BBC News Online:* Facial recognition database 'risks targeting innocent people', 14 September 2018 [viewed on 10/02/2018]. Available from http://www.bbc.co.uk/news/uk-41262064

[34] *Science and Technology Committee:* Oral Evidence – Biometrics Strategy and Forensic Services, HC 800, 6 February 2018. Available from http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/biometrics-strategy-and-forensic-services/oral/78113.html

[35] Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

[36] Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

[37] EWHC 1681 (Admin) ('*RMC*')

[38] Press Association: 'Custody image' deletion request figures revealed, 12 February 2018 [viewed on 12/02/2018]. Available from http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.html

[39] Arrangements for storing millions of 'custody images' may be unlawful, MP says – 14 February 2018 http://www.dailymail.co.uk/wires/pa/article-5389875/Arrangements-storing-millions-custody-images-unlawful-MP-says.html

[40] The Surveillance Camera Commissioner's Annual Report 2016/17

[41] Commissioner for the Retention and Use of Biometric Material, Paul Wiles – *Annual Report*, September 2017, para. 301-5

[42] *BBC News Online*: Download festival: Leicestershire Police defend facial recognition scans, 15 June 2015 {viewed on 01/02/2018]. Available from http://www.bbc.co.uk/news/uk-england-leicestershire-33132199

[43] *Press Association*: Notting Hill Carnival patrolled by police 'super-recognisers' in crime crackdown, 28 August 2016 [viewed on 05/02/2018]. Available from https://www.telegraph.co.uk/news/2016/08/28/face-recognition-police-to-scan-notting-hill-carnival/

[44] *Metropolitan Police News*: Statement from police commander for Notting Hill Carnival 2016, 30 August 2016. Available from http://news.met.police.uk/news/statement-from-police-commander-for-notting-hill-carnival-2016-182480

[45] Dodd, Vikram; *The Guardian*: Met police to use facial recognition software at Notting Hill carnival, 5 august 2017. Available from https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival

[46] Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

[47] Metropolitan Police, Freedom of Information Request response ref. 2018030000548 to Big Brother Watch (available on our website)

[48] Townsend, Mark; *The Guardian:* Police to use facial-recognition cameras at Cenotaph service, 12 November 2017. Available from https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph

[49] Fixated Threat Assessment Centre http://www.fixatedthreat.com/ftac-welcome.php

[50] Metropolitan Police, Freedom of Information Request response ref. 2018030000548 to Big Brother Watch (available on our website)

[51] Letter from Baroness Williams to the Chair of the Science and Technology Committee, 28 March 2018 https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf

[52] South Wales Police and Crime Commissioner, Medium Term Financial Strategy2017-2021https://pcclivewww.blob.core.windows.net/wordpress-uploads/2016-12-28-Final-Medium-Term-Financial-Strategy.pdf

[53] South Wales Police, Freedom of Information Request response 268/18 to Big Brother Watch (available on our website)

[54] South Wales Police: Press Release, 4 December 2017 https://motorpointarenacardiff.co.uk/news-and-alerts/facial-recognition-technology-partnership-south-wales-police

[55] Apple, Emily; *The Canary*: South Wales Police under fire for using facial recognition technology against protesters, 29 March 2018 [viewed on 03/04/2018]. Available from https://www.thecanary.co/uk/2018/03/29/south-wales-police-under-fire-for-using-facial-recognition-technology-against-protesters/

[56] Professional Security, 28 March 2018. Available from http://www.professionalsecurity.co.uk/news/interviews/new-ring-of-steel-proposed/

[57] Louise Cooper, Huddersfield Daily Examiner, 26 August 2017, How new-style CCTV could help find missing people more quickly. Available from https://www.examiner.co.uk/news/west-yorkshire-news/how-new-style-cctv-could-13532881

[58] Louise Cooper, Huddersfield Daily Examiner, 26 August 2017, How new-style CCTV could help find missing people more quickly. Available from https://www.examiner.co.uk/news/west-yorkshire-news/how-new-style-cctv-could-13532881

[59] SCC, SCC Wins Police Contract to Provide Post-Event Video Forensics and Analysis for Law Enforcement and Security, 24 January 2018. Available from https://www.scc.com/news/scc-awarded-contract-provision-post-event-video-forensics-analysis-law-enforcement-security/

[60] NPS, CONNECT Product Summary. Available from https://marketing.northgateps.com/acton/attachment/17827/f-0261/1/-/-/-/-/CONNECT%20Policing.pdf

[61] Sam Trendall, Public Technology, NEC agrees £475m deal to buy Northgate Public Services, 9 January 2018. Available from https://www.publictechnology.net/articles/news/nec-agrees-%C2%A3475m-deal-buy-northgate-public-services

[62] Catriona Stewart, Evening Times, Haghill gang: CCTV cameras will crack down on violence and crime, 31 March 2018. Available from http://www.eveningtimes.co.uk/news/16129720.Housing_bosses_have_new_weapon_in_fight_against_Haghill_gang/

[63] Rietzschel, Antonie, *Süddeutsche Zeitung* [online]: Bitte lächeln, Sie werden überwacht, 1 August 2017 [viewed 12/02/2018]. Available from: http://www.sueddeutsche.de/digital/ueberwachung-in-berlin-bitte-laecheln-sie-werden-ueberwacht-1.3611953

[64] Prantl, Heribert, *Süddeutsche Zeitung* [online]: Die optische Rasterfahndung, 1 August 2017 [viewed 12/02/2018]. Available from: http://www.sueddeutsche.de/politik/gesichtserkennung-die-optische-rasterfahndung-1.3611830

[65] *Der Spiegel* [online]: Berliner Südkreuz - De Maizière verlängert umstrittene Tests zur Gesichtserkennung, 15 December 2017 [viewed 12/02/2018]. Available from: http://www.spiegel.de/netzwelt/netzpolitik/bahnhof-berlin-suedkreuz-testlauf-zur-gesichtserkennung-wird-verlaengert-a-1183528.html

[66] *Deutscher Anwalt Verein* [online]: PM 9/17: Deutscher Anwaltverein: Gesichtserkennung in Bahnhöfen greift massiv in Grundrechte ein. Pressemitteilung zum Start des Pilotprojekts Gesichtserkennung am Berliner Bahnhof Südkreuz, 1 August 2017 [viewed 22/03/2018]. Available from: https://anwaltverein.de/de/newsroom/pm-9-17-deutscher-anwaltverein-gesichtserkennung-in-bahnhoefen-greift-massiv-in-grundrechte-ein

[67] Original quote from German: "Dieses Zusammenspiel aus technischen und rechtlichen Neuerungen stellt den Schutz der Freiheitsrechte vor neue Gefahren", betonte der DAV-Präsident.

[68] Vincent, James, *The Verge* [online]: Moscow says its new facial recognition CCTV has already led to six arrests, 28 September 2017. [viewed 20/02/2018]. Available from https://www.theverge.com/2017/9/28/16378164/moscow-facial-recognition-cctv-arrests-crime-surveillance

[69] Mezzofiore, Gianluca, *Mashable UK* [online]: Moscow's facial recognition CCTV network is the biggest example of surveillance society yet, 28 September 2017. [viewed 20/02/2018]. Available from https://mashable.com/2017/09/28/moscow-facial-recognition-cctv-network-big-brother/#_atYz8NXR8qX

[70] Khrenikov, Ilya, *Bloomberg Technology* [online]: Moscow Deploys Facial Recognition to Spy on Citizens in Streets, 28 September 2017. [viewed 15/03/2018] Available from https://www.bloomberg.com/news/articles/2017-09-28/moscow-deploys-facial-recognition-to-spy-on-citizens-in-streets

[71] Phillips, Tom; *The Guardian* [online]: China testing facial-recognition surveillance system in Xinjiang – report, 18 January 2018 [viewed 02/02/2018]. Available from: https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report

[72] Liu, Joyce, *BBC News Online*: In Your Face: China's all-seeing state, 10 December 2018. Available from http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

[73] Francis Chan, Tara, *Business Insider*: 16 parts of China are now using Skynet, the facial recognition tech that can scan the country's entire population in a second, 27 March 2018. Available from https://www.businessinsider.com.au/china-facial-recognition-technology-works-in-one-second-2018-3

[74] Liao, Shannon, *The Verge*: Chinese police are expanding facial recognition sunglasses program, 12 March 2018. Available from https://www.theverge.com/2018/3/12/17110636/china-police-facial-recognition-sunglasses-surveillance

[75] Oberhaus, Daniel; *Motherboard* [online]: China Is Using Facial Recognition Technology to Send Jaywalkers Fines Through Text Messages, 28 March 2018 [viewed 28/03/2018]. Available from: https://motherboard.vice.com/en_us/article/wj7n74/china-jaywalking-facial-recognition-camera

[76] Phillips, Tom; *The Guardian* [online]: China testing facial-recognition surveillance system in Xinjiang – report, 18 January 2018 [viewed 02/02/2018]. Available from: https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report

[77] Phillips, Tom (2018): China testing facial-recognition surveillance system in Xinjiang – report https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report

[78] *Human Rights Watch* [online]: China: Big Data Fuels Crackdown in Minority Region, 26 February 2018 [viewed 27/02/2018]. Available from: https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

[79] Draper, Kevin; *The New York Times*: Madison Square Garden Has Used Face-Scanning Technology on Customers, March 13 2018. Available from https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html

[80] Garvie, Clare; Bedoya, Alvaro M.; Frankle, Jonathan; *Georgetown Law Center on Privacy and Technology*: The Pertual Line-Up – Unregulated Police Face Recognition in America, p.2, 18 October 2016. Available from https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

[81] Waddell, Kaveh; *The Atlantic*: Half of American Adults Are in Police Facial-Recognition Databases, 19 October 2016 [viewed on 15/03/2018]. Available from https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk | @bbw1984