BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch Briefing for the Westminster Hall debate on Facial recognition and the biometrics strategy on 1st May 2019

April 2019

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation. We hold to account those who fail to respect our privacy, and campaign to give individuals more control over their personal data. We produce unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Contact

Silkie Carlo

Director

Direct line: 020 7340 6042

Email: silkie.carlo@bigbrotherwatch.org.uk

Griff Ferris

Legal & Policy Officer

Direct line: 020 7340 6074

Email: griff.ferris@bigbrotherwatch.org.uk

Westminster Hall debate: Facial recognition and the biometrics strategy

Wednesday 1st May 2019, 2.30 – 4.00pm

The Member sponsoring the debate is Darren Jones MP.

Contents

Summary

We urge Members of Parliament to:

- call on police to immediately stop **using live facial recognition surveillance**, and
- call on the Home Office to make a firm commitment to **automatically remove the thousands of images of unconvicted individuals from the custody image database.**

Introduction

In this briefing, we examine one of the most pressing issues in the area of civil liberties and biometrics in the UK - police forces' use of live facial recognition surveillance technology. We welcome the opportunity to provide briefing ahead of this debate and seek to inform parliamentarians of the significant risks live facial recognition surveillance poses to human rights and the rule of law in the UK.

- **A threat to freedom**: The emergence of live facial recognition surveillance by police in England and Wales poses **one of the most serious threats to civil liberties of recent years**. This China-style mass surveillance tool risks turning CCTV cameras into biometric checkpoints and citizens into walking ID cards.

- **Incompatible with human rights:** We explore the impact of live facial recognition surveillance on human rights in the UK and explain why such **biometric checkpoints cannot be compatible with the rights framework.**

- **Discriminatory:** Furthermore, research has found that many live facial recognition algorithms have **discriminatory effect, disproportionately misidentifying black people and women.**

- **No law, policy or safeguards:** Parliament has never passed a law enabling police use of facial recognition surveillance. T**here are no laws and no safeguards** regulating this alarming expansion of surveillance in the UK.

- **Ineffective:** Over recent years, live facial recognition has proven to be **dangerously inaccurate**, producing high numbers of 'false positive' matches. Police have accrued **thousands of false positive matches** of members of the public whose photos have been subsequently taken and, for a period, stored.

- **Over-policing:** Big Brother Watch has witnessed **innocent members of the public being misidentified, stopped and searched – including a 14 year old black boy in school uniform.** We have also witnessed people being **stopped and forced to show identification**, and in one case even **fined**, for wearing hooded jackets or having scarves covering their chins in winter weather.

Secondly, we raise the issue that **the custody image database contains hundreds of thousands of innocent people's images**, likely unlawfully.

- The database contains 23 million images, up from 19 million images in 2016. 10 million of these images are searchable using facial recognition technology.[1]

- The storage of innocent people's images was ruled unlawful by the High Court in 2012.[2] However, no effort has yet been made to remove unconvicted people's images from the database, and the police use images from this database at deployments of live facial recognition.

[1] Paul Wiles in oral evidence to the Science and Technology Committee, 19 March 2019, Q83: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf

[2] RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] EWHC 1681 (Admin)

About facial recognition

Facial recognition technology measures and matches unique facial characteristics for the purposes of biometric surveillance or identification.

There are two types of facial biometric recognition:

- **Facial matching or 'static' facial recognition:** this is the matching of an isolated, still image of an individual against a database. This is used at borders with biometric passports and by police to match images of suspects against images on the Police National Database.
- **Live facial recognition:** this technology matches faces on live surveillance camera footage against a database (such as the custody image database, or a subsidiary 'watchlist') in real time.

South Wales Police describes the live facial recognition process as follows:

> *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.***

The technology police in the UK use is called NeoFace Watch, provided by the Japanese conglomerate NEC. It has the capability to scan and identify as many as 300 faces a second, or 18,000 people a minute.[3]

NEC boasts of the "*distinct advantages*" that its facial recognition technology offers due to its "*non-contact process*" that "*does not require interacting with the person*" who is photographed and identified.[4]

[3] https://crimeandsecurity.org/feed/afr

[4] NEC website, *Putting More Than Just a Name to a Face* https://www.nec.com/en/global/solutions/safety/face_recognition/index.html

The use of live facial recognition technology in UK policing

In the UK, live facial recognition surveillance technology has been deployed by the Metropolitan Police, South Wales Police, Greater Manchester Police, Leicester Police and Humberside Police.

Since 2016, the Metropolitan Police and South Wales Police have deployed this surveillance technology prolifically: at sports matches, concerts, shopping centres and high streets, Notting Hill Carnival, Remembrance Sunday – and even a peaceful demonstration. South Wales Police ihas received £2m in funding from the Home Office to lead the deployment of automated facial recognition.[5]

In 2018, Greater Manchester Police deployed the technology at the Trafford Centre shopping centre for a period of 6 months in 2018 biometrically scanning an estimated 15 million people, before the Surveillance Camera Commissioner intervened.[6]

As of January 2019, the trials had so far cost the Metropolitan Police over £220,000 just in material costs, not including the significant costs of teams of uniformed and plainclothes officers in attendance at each deployment.[7]

[5] 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

[6] Working together on automatic facial recognition – Tony Porter, Surveillance Camera Commissioner, 10 October 2018 - https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/

[7] https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-met-arrests-london-cost-false-positives-accuracy-a8723756.html

THE ISSUES

An unprecedented erosion of civil liberties

This is a turning point for facial recognition and civil liberties in the UK. If police decide to press ahead with their lawless use of facial recognition surveillance, the floodgates will be opened for ever more uses of the authoritarian technology to track and monitor members of the public.

In advance of this debate, Big Brother Watch successfully reached our crowdfunding goal of £10,000, thanks to 284 backers, to bring a legal challenge against the Metropolitan Police and Home Office's lawless use of live facial recognition surveillance in public places. Should police decide to pursue live facial recognition, we will seek to proceed with our legal challenge.

As awareness increases, public opposition to this China-style mass surveillance tool is rapidly growing. For a nation that opposed ID cards and a national DNA database, the idea of citizens being turned into walking ID cards is the very antithesis of British notions of democratic freedom.

The threat to human rights

A threat to the right to privacy

Live 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 live facial recognition with CCTV cameras in public spaces appears to fail both of these tests.

Live 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 96% of matches inaccurately identifying innocent people.

It is plainly disproportionate to deploy a public surveillance 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 live 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.*"[8]

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 Baroness Jones of Moulsecoombe in 2018 – 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 spoke to realised what was already going on. Some were horrified, some were puzzled and every one of them had questions and worries."*[9]

The Surveillance Camera Commissioner has said that "*overt use of such advancing technology (AFR) [live facial recognition] is arguably more invasive than some covert surveillance techniques*."

> *Case study – 15 million people potentially scanned to find just 53 people*
>
> Greater Manchester Police, in conjunction with the owners of a major shopping centre, used live facial recognition on visitors to the centre for a period of 6 months. It is estimated that 15 million people visited the Trafford Centre during that time, many of whom would have been scanned by the facial recognition cameras. However, this was all for the purpose of finding just 53 individuals.
>
> The Surveillance Camera Commissioner stated that the deployment was extremely disproportionate as "compared to the scale and size of the processing of all people passing a camera, the group they might hope to identify was minuscule".[10]

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

[9] 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

[10]https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/

Even industry leaders in facial recognition technology have warned about the potential dangers of the technology when used by authorities. Researchers from Google and Microsoft warned about "*oppressive*" potential of the technology,[11] and Microsoft's President Brad Smith stated that "*the use of facial recognition by a government for mass surveillance can encroach on democratic freedoms*" and "*lead to new intrusions into people's privacy.*"[12]

Proportionality is a particular concern in relation to live 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. Proportionality concerns are significantly heightened in the context of the authorities' intentions for the technology. Police have indicated that they intend to implement live facial recognition in future throughout the UK's enormous existing CCTV network, which numbers 6 million cameras:

> *"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."*[13]

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 live 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.

[11] https://www.telegraph.co.uk/technology/2018/12/07/microsoft-president-calls-new-rules-facial-recognition-technology/

[12] https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

[13] 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/)

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*".[14]

Many of the people we have spoken to at trials of live facial recognition were shocked and felt both uncomfortable and targeted.

Discrimination

There are serious concerns about the discriminatory impact of live facial recognition surveillance. A number of high profile studies have found that commercial facial recognition algorithms, including those used by some police forces, have demographic accuracy biases – that is that they misidentify some demographic groups at higher rates than others.

In March 2017, the US Government Accountability Office found that facial recognition algorithms used by the FBI are inaccurate almost 15% of the time and are more likely to misidentify female and black people.

The American Civil Liberties Union demonstrated this bias by using Amazon's 'Rekognition' facial recognition software used by several US police forces to compare members of the US House of Representatives to a custody image database, resulting in a number of misidentifications. The false matches were disproportionately of people of colour.

A 2018 study by the Massachusetts Institute of Technology (MIT) found that commercial facial recognition technology, including those created and sold by Microsoft and IBM, misidentified dark-skinned women up to 35% of the time compared to 1% for light-skinned men.[15] A follow up study by MIT in 2019 found that

[14] 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)

[15] http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

> Amazon's 'Rekognition' software mistook women for men 19% of the time, and darker-skinned women 31% of the time.[16]
>
> These biases could be coded into the software by programmers, albeit unintentionally, and/or due to an under-representation of black people and women in the training datasets used to develop the software.

The Biometrics and Forensics Ethics Group warned that UK police's use of live facial recognition technology has the "*potential for biased outputs and biased decision-making on the part of system operators*".[17]

In the Metropolitan Police's recent written evidence to the Science and Technology Committee, the force stated:

> "*The MPS is cognisant of the concern over the system response with respect to different demographics. We are working to further mitigate potential impact of this within the operational context, where it should be noted, additional checks and balances are in place and the final decision is by a human operator."*[18]

This suggests the police has noticed the need to "mitigate" the discriminatory impact, despite this never having been formally tested by them. They also repeat the claim that a human review of a match prior to stopping someone can mitigate the risk of ethnic minorities disproportionately being matched and misidentified, which is plainly an untrue and unacceptable position. They continued, "*The MPS plans to continue to test demographic differences" -* a long overdue and confusing commitment, given that MPS has never before tested demographic differences and has thus far resisted all of our calls to do so.

That said, our analysis and the analysis of many human rights groups around the world is that even if live facial recognition technology improves in demographic and general accuracy it remains too great a risk to civil liberties, dangerously imbalances power between citizen and state, and constitutes a fundamental threat to the right to privacy.

[16] http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

[17] Biometrics and Forensics Ethics Group, Interim report, February 2019

[18] Written evidence submitted by Metropolitan Police Service (WBC0005), 19 March 2019: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97851.pdf

No law

There is no legal basis for the police's use of live facial recognition surveillance.

When Layla Moran MP posed a written question to the Home Office about current legislation regulating "the use of CCTV cameras with facial recognition and biometric tracking capabilities", Nick Hurd MP (Minister for Policing, responding for the Home Office) answered: "There is no legislation regulating the use of CCTV cameras with facial recognition". The Metropolitan Police have also acknowledged that "There is currently no specific legal framework in the use of this technology."[19]

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

The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras in England and Wales. There is no reference to facial recognition in the Protection of Freedoms Act, although it provides the statutory basis for public space surveillance cameras.

Section 30 of the Act required the Secretary of State to issue the Surveillance Camera Code of Practice. There are just three passing mentions in the Surveillance Camera Code of Practice to facial recognition, which make vague statements as to justification and proportionality. This lack of meaningful regulation, guidance or safeguards cannot be considered a suitable regulatory framework for a technology as potentially intrusive as live facial recognition.

Police have claimed that their use of live facial recognition is regulated by the Protection of Freedoms Act 2012 and the Data Protection Act 2018. As with the Protection of Freedoms Act 2018, there is not a single mention of live facial recognition in the Data Protection Act 2018.

The Surveillance Camera Commissioner said in recent evidence to the Science and Technology Committee that:

[19] https://www.london.gov.uk/press-releases/mayoral/independent-panel-delivers-report-on-polices-use

> "*The Data Protection Act 2018 alone does not provide a basis in law for use of this technology nor does the completion of a Data Protection Impact Assessment* (DPIA)."[20]

Meanwhile, the Biometrics Commissioner stated that "*PoFA is not generic legislation covering all biometrics used by the police*" and therefore that "t*he use by the police of these second generation biometrics is not currently governed by any specific legislation*."[21] The Commissioner added that "*each use of biometric information the balance between public benefit and individual privacy (proportionality) should be decided by Parliament.*"[22]

The Information Commissioner has expressed serious concern about the police's use of live facial recognition in the absence of a legal basis:

> *"The Commissioner is so concerned with the practices in some areas that a priority investigation has been opened to understand and investigate the use of AFR by law enforcement bodies in public spaces. This will include considering the legal basis, the necessity, proportionality and justification for this intrusive processing."*[23]

The police's use of live facial recognition has never been scrutinised or considered by the House of Commons. The Home Office said in a letter to the House of Commons Science & Technology Committee in late 2017 that "*A decision to deploy facial recognition systems is an operational one for the police*."[24] However, this is a rights-altering technology that will significantly erode privacy and civil liberties in the UK. We believe that live facial recognition surveillance is incompatible with the Human Rights Act and that parliamentary consideration is urgently required – particularly given the technology's significant and unique impact on rights in the UK.

[20] Surveillance Camera Commissioner evidence to the Science and Technology Committee, March 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97777.html

[21] Biometrics Commissioner, Annual Report 2017 (June 2018)

[22] Biometrics Commissioner, Annual Report 2017 (June 2018)

[23] Information Commissioner's Office evidence to the Science and Technology Committee, March 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

[24] Letter from Baroness Williams, Minister for the Home Office, to the Chair of the Science and Technology Committee, 30 November 2017 ()

No policy

Live facial recognition surveillance is fundamentally incompatible with the right to privacy and freedom of expression, according to our analysis. It has no place on our streets.

However, its negative impact on freedoms in the UK is exacerbated by the lawless way in which its use by police has evolved.

There is no policy or guidance regulating the use of live facial recognition surveillance. Which databases can be matched against, which images are captured and stored, who can access those images, how long they are stored – are all questions without answers. Extremely sensitive policy decisions are being left to the discretion of police, or deferred to the legal challenges brought by us at Big Brother Watch and Liberty (the Metropolitan Police recently stated that "*Future Judicial Reviews could also provide further direction for law enforcement in using this technology"*).[25]

> Nor is there any policy limiting the purposes for which live facial recognition surveillance can be used.
>
> *Case study – Innocent people with mental health problems*
>
> At Remembrance Sunday in November 2017, the Metropolitan Police used live facial recognition to match against a dataset of 'fixated individuals' – people who frequently contact public figures and are highly likely to suffer mental health issues, but who were not suspected of or wanted for any criminal activity. No mental health support or advocacy groups were consulted or informed. This non-criminal application of facial recognition technology resulted in a so-called 'fixated individual' being identified and subsequently ejected from the ceremony by police. The use of this authoritarian technology to target people suffering mental ill health is an unprecedented infringement of civil liberties and could have serious adverse health effects.

The Government promised a Biometrics Strategy in 2013. In June 2018, 5 years later, a Biometrics Strategy was published that was widely criticised for its lateness and brevity. While the strategy name-checked 'facial images', 'facial matching' and 'automated

[25] Written evidence submitted by Metropolitan Police Service (WBC0005), 19 March 2019: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97851.pdf

facial recognition (AFR)', it provided no clarity on the enduring policy vacuum, merely stating that "looking further ahead, we will consider the use of AFR [live facial recognition] for verifying identity and identifying known criminals of interest". The Biometric Strategy erroneously states that the use of AFR technologies is "governed by...PACE [the Police and Criminal Evidence Act 1984]."[26]

The Strategy announced that the Home Office "*will establish a new oversight and advisory board to coordinate consideration of law enforcement's use of facial images and facial recognition systems*" and will provide policy recommendations regarding the use of facial biometrics.[27] The Biometric Strategy also stated that Data Protection Impact Assessments will be conducted prior to the use of any new biometric technology – something that is already a legal requirement and that the Surveillance Camera Commissioner has said does not provide legal legitimacy for the use of such systems.

The Biometric Strategy also stated that the Home Office would "*ensure that standards are in place to regulate the use of [live facial recognition] before it is widely adopted for mainstream law enforcement purposes*." By this point, June 2018, the Metropolitan Police had already been using live facial recognition for two years, South Wales Police for a year, and Greater Manchester Police were beginning to scan millions of people at the Trafford Centre. This is a largely meaningless policy statement.

No effective oversight

Police have said they will seek oversight of their use of live facial recognition from the Information Commissioner's Office, Biometrics Commissioner, Surveillance Camera Commissioner.

However, the Commissioners have questioned who actually has oversight over the police's use of this surveillance technology. The Surveillance Camera Commissioner questioned in his 2016 report: "C*larity regarding regulatory responsibility is an emerging issue, for example in automatic facial recognition use by police – which regulator has responsibility*"[28] and has said that the Government "*appears to leave oversight and management of this process solely to the police*".[29] The Commissioner said he hoped the the Biometric Strategy would "*provide*

[26] Home Office Biometrics Strategy (June 2018)
[27] Home Office Biometrics Strategy (June 2018)
[28] Review of the impact and operation of the Surveillance Camera Code of Practice –Surveillance Camera Commissioner, Feb 2016, p.15
[29] Surveillance Camera Commissioner, Annual Report 2016/17 (January 2018)

much needed clarity over respective roles and responsibility" in relation to live facial recognition surveillance. He was to be disappointed, as the Biometric Strategy gave no such clarity.

In 2017, the Biometrics Commissioner said that the trials required "*independent oversight to reassure the public*".[30] Meanwhile, the Information Commissioner's Office is investigating the police's trials of live facial recognition surveillance.

The Biometrics Commissioner has rightly said that "*deciding what is proportionate should not be left to those who seek to benefit from the use of the biometric.*"[31]

A new Law Enforcement Facial Images and Biometrics Oversight and Advisory Board met for the first time in July 2018. It consists overwhelmingly of police, including the very members of the Metropolitan Police and South Wales Police who are using live facial recognition surveillance, raising serious questions as to its impartiality and ability to provide meaningful and effective oversight.

Ultimately, the Commissioners have seriously questioned whether the police should be using live facial recognition for general surveillance at all. The Biometrics Commissioner has made his view on the police's continued use of live facial recognition clear, stating that "*This would not be a sensible time to start routinely deploying [live facial recognition] operationally, a number of questions still need to be answered.*"[32]

In evidence to the Science and technology Committee in March 2019, the Information Commissioner's Office said that:

> "*The Committee's view was that facial recognition technology should not generally be deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved. The Commissioner is concerned that this has not been fully addressed and it is not yet clear how the 'oversight board' will address these issues.*"[33]

[30] https://www.gov.uk/government/news/metropolitan-polices-use-of-facial-recognition-technology-at-the-notting-hill-carnival-2017

[31] Biometrics Commissioner, Annual Report 2017 (June 2018)

[32] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.html

[33] Information Commissioner's Office evidence to the Science and Technology Committee, March 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

This lack of meaningful oversight has resulted in some extremely concerning uses of live facial recognition surveillance.

> *Case study – live facial recognition used at a peaceful protest*
>
> In March 2018, South Wales Police used live facial recognition surveillance at a lawful and peaceful demonstration at an arms fair in Cardiff. 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. In the online discourse around the event, Big Brother Watch witnessed the chilling effect this had on demonstrators who felt they were unfairly targeted and surveilled.[34]

[34]https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Inaccurate and ineffective: new statistics

Live facial recognition surveillance is currently a dangerously inaccurate and ineffective tool. It has resulted in the misidentification of hundreds of innocent people as criminals, with many people being wrongly stopped and forced to identify themselves – including schoolchildren. Many people have also been stopped for covering their faces while going past the live facial recognition cameras.

There has been very little transparency from either the Metropolitan Police or South Wales Police about their use of live facial recognition, but Big Brother Watch has published statistics provided by the Metropolitan Police themselves in response to Freedom of Information requests.

- In **May 2018** we revealed that the Metropolitan Police's use of live facial recognition in public spaces was **98% inaccurate** – it identified people correctly only 2% of the time.[35] We also revealed that South Wales Police's live facial recognition was **inaccurate 91% of the time** and had resulted in the misidentification of 2,451 people.
- **NEW:** Overall since 2016, the most up to date figures obtained via freedom of information requests show that the Metropolitan Police's live facial recognition surveillance has been **96% inaccurate.**
- **NEW:** In its entire history of deployments since 2016, the most up to date figures obtained via freedom of information requests from the police show that **the Metropolitan Police's surveillance technology has resulted in only 3 arrests**, making over 120 incorrect matches. This already risks arbitrary policing; but used on a mass scale, the error rate would be untenable.

The Biometrics and Forensics Ethics Group, set up to oversee the legitimacy of new biometrics, concluded in an interim report in February 2019 that "*There are a number of questions about the accuracy of live facial recognition (LFR) technology*".[36]

[35] https://bigbrotherwatch.org.uk/all-media/dangerous-and-inaccurate-police-facial-recognition-exposed-in-new-big-brother-watch-report/
[36] Biometrics and Forensics Ethics Group, Interim report, February 2019

Overpolicing

In our observations of the Metropolitan Police's trials, we witnessed the following individuals being treated unfairly by police in the course of misidentifications and wrongful stops.

Case study 1

A 14 year old black school child, wearing school uniform, was wrongly identified by the facial recognition system, and subsequently surrounded by four plainclothes police officers. He was pulled onto a side-street, his arms held, questioned, asked for his phone, and even fingerprinted. He was released after ten minutes when police realised they had the wrong person. The child appeared frightened and said he felt was being harassed by police.

Case study 2

A man was stopped for covering his mouth and chin with his jacket after seeing facial recognition signs and expressing his objection to the deployment. His reaction was observed by a plainclothes police officer who followed him and radioed through to other officers to make a stop. Police demanded his ID and the man complied. However, protesting against the facial recognition cameras, he was issued with a £90 public order fine for 'shouting profanities in public view'. The man was not wanted for any crime, and after being fined, he was released.

Case study 3

A young man was stopped by two police officers for covering his mouth and chin with his scarf as he walked past a police live facial recognition van. He was trying to keep warm on a freezing cold day. The two police officers asked for his details and checked his ID against the police database, letting him go after he didn't come up as wanted. He was distressed at having been stopped and made late for work. He was not aware of the live facial recognition surveillance or what it was.

Case study 4

On the coldest day of the year, a young black boy in school uniform, wearing a hooded jacket, was stopped and forced to show his ID as he was not visible to the facial recognition cameras. His friend told us he was distressed and had felt harassed.

Custody images and facial recognition

There are currently 23 million images on the police's custody image database, held on the Police National Database. In 2016, there were 19 million images on the database. This is a worrying increase of 4 million images in just 3 years. 10 million of these custody images are searchable using facial recognition technology.[37]

Government says the retention of such images is governed by the MoPI regime (management of police information) as well as data protection and ECHR considerations. Images can be held for a minimum of six years with retention renewed indefinitely.

The storage of innocent people's images was ruled unlawful by the High Court in 2012.[38] However, no effort has yet been made to remove unconvicted people's images from the database, the police still hold these images, and they use images from this database at deployments of live facial recognition.

In February 2017, following a 'Custody Image 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. We are aware of only 34 successful requests.

In practice, there has been no change to this likely unlawful policy. The Home Office clearly needs to delete the thousands of images stored of innocent people.

The Biometrics and Forensics Ethics Group (BFEG or EG) has also commented:

> *"The review did not align with the EG's previous advice,* ***that the retention times*** *directed in the Protection of Freedoms Act 2012 f****or the retention of DNA samples and fingerprints should also be applied to the retention of custody images"***[39]

The Biometrics Commissioner said at the time of Custody Image Review "*I was not at all sure this would meet further court challenges. I still think that.*"[40] The Commissioner said in March

[37] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.html

[38] *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)

[39] Annual Report – Biometrics and Forensics Ethics Group (prev. National DNA Database Ethics Group (NDNADEG), October 2017, pg. 9

[40] https://parliamentlive.tv/Event/Index/f9d3913e-b5c2-41e6-8452-de80f49e85e9

2019 that "*I am not sure that the legal case is strong enough and that it would withstand a further court challenge*."[41]

Our campaign

In May 2018, we brought together 15 human rights and race equality groups, MPs and Lords including David Lammy MP, Sir Edward Davey MP, Baroness Jenny Jones and Lord Strasburger to sign a joint statement raising concerns about the impact live facial recognition would have on individuals' rights to a private life and freedom of expression and the potential for discriminatory impact, and calling for an immediate end to its use for public surveillance.[42]

The organisations included Big Brother Watch, Liberty, the Police Action Lawyers Group, the Institute of Race Relations, Race Equality Foundation, Runnymede Trust, Race on the Agenda, Article 19, Index on Censorship, Netpol, The Monitoring Group, Tottenham Rights, and the Football Supporters Federation.

In July 2018, Big Brother Watch and Baroness Jenny Jones launched a legal challenge against the Metropolitan Police and the Home Secretary on the basis that their use of live facial recognition had infringed people's Article 8 right to privacy and Article 10 rights to freedom of expression and association. We await the outcome of the Metropolitan Police's decision on their future use of live facial recognition, and stand ready to proceed with the challenge.[43]

CONCLUSION

We urge Members of Parliament to:

- call on police to immediately stop **using live facial recognition surveillance**, and
- **call on the Home Office to make a firm commitment to automatically remove the thousands of images of unconvicted individuals from the custody image database.**

[41] https://parliamentlive.tv/Event/Index/f9d3913e-b5c2-41e6-8452-de80f49e85e9

[42] Big Brother Watch, Liberty, Article 19, Runnymede Trust https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/

[43] https://www.crowdjustice.com/case/face-off/