BIG BROTHER WATCH

Big Brother Watch Briefing on facial recognition surveillance

June 2020

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Direct line: 020 7340 6042

Email: silkie.carlo@bigbrotherwatch.org.uk

Facial recognition surveillance

Contents

Summary....4

About facial recognition surveillance....6

The use of facial recognition surveillance in policing....7

Collaboration between police and private companies....7

THE ISSUES....9

An unprecedented erosion of civil liberties....9

The threat to human rights....9

Innocent people targeted....13

Discrimination....14

No law....16

No policy.... 17

No effective oversight....19

Inaccurate and ineffective: new statistics....21

Overpolicing: case studies....23

Custody images and facial recognition....25

Opposition to facial recognition surveillance....26

SUMMARY

In this briefing, we examine one of the most pressing issues in the area of civil liberties and biometrics in the UK – police and private company use of live facial recognition surveillance technology.

We are seeking 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 use of live facial recognition surveillance by police in England and Wales represents **an enormous expansion of the surveillance state** and **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.**
- **Innocent people targeted:** police have used this intrusive surveillance to monitor and track **innocent people with mental health problems**, **peaceful protestors**, and their own operating procedures state that **people with no criminal record can be targeted and tracked** by live facial recognition surveillance.
- **Discriminatory:** research has found that many live facial recognition algorithms have **discriminatory effect, disproportionately misidentifying people of colour and women.**
- **No law, policy or safeguards:** Parliament has never passed a law enabling police use of facial recognition surveillance. There 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 thousands of misidentifications, resulting in **innocent people being stopped**, asked to prove they aren't wanted criminals, and even searched, on many occasions.
- **Over-policing:** Big Brother Watch has witnessed **innocent members of the public being misidentified, stopped and searched – including a 14 year old black child 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.

- **Significant opposition:**

  26 rights, race equality and technology groups, as well as **cross party MPs** including David Davis MP, Diane Abbott MP, Ed Davey MP, and Caroline Lucas MP, have **called for an "immediate stop" to facial recognition surveillance**.[1]

  The **Equalities and Human Rights Commission** has said the **legal framework is insufficient** and its use may be **disproportionate**.[2] The **Scottish Parliament** has also **refused to allow Scottish police to use live facial recognition**, while **Police and Crime Commissioners** have called it **"a step too far"**.[3] We have also brought a **legal challenge** against the Metropolitan Police and the Home Office, while another challenge against South Wales Police is to be considered by the Court of Appeal in June 2020.

Secondly, we raise the issue that **the custody image database contains hundreds of thousands of innocent people's images**, likely unlawfully, which can be used with live facial recognition surveillance:

- The database contains 23 million images, up from 19 million images in 2016. 10 million of these images are searchable using facial recognition technology.[4]
- The storage of innocent people's images was ruled unlawful by the High Court in 2012,[5] and the European Court of Human Rights ruled in February 2020 that even convicted people's photos and biometric data cannot be stored indefinitely.[6] 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 https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019.pdf
2https://www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf
3https://www.theguardian.com/technology/2020/jan/08/facial-recognition-at-south-wales-derby-a-step-too-far-says-police-chief
4 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
5 *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)
6 *Gaughran v the United Kingdom* (Application No. 45245/15) [2020] ECtHR, 13 February 2020 (http://hudoc.echr.coe.int/eng?i=001-200817)

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.**

ABOUT FACIAL RECOGNITION SURVEILLANCE

Facial recognition technology measures and matches unique facial characteristics ('biometrics') 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 surveillance:** 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.[7]

NEC boasts of the "*distinct advantages*" that its facial recognition surveillance technology offers due to its "*non-contact process*" that "*does not require interacting with the person*" who is photographed and identified.[8]

7https://crimeandsecurity.org/feed/afr
8 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 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 has received £2m in funding from the Home Office to lead the deployment of automated facial recognition.[9]

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.[10]

As of February 2020, the trials had so far cost the Metropolitan Police over £240,000 just in material hardware and software costs, not including the significant costs of teams of uniformed and plainclothes officers in attendance at each deployment.[11] Police have refused to provide the full costs.

The Metropolitan Police announced on 24th January 2020 that it was rolling out the technology operationally across London.[12]

Collaboration between police and private companies

Several UK police forces have also collaborated with private companies using facial recognition surveillance.

In Sheffield, South Yorkshire Police shared images with Meadowhall Shopping Centre during a secret trial of facial recognition surveillance.[13] Millennium Point conference centre in Birmingham stated in their privacy policy that they used facial recognition "at the request of law enforcement",[14] which they then subsequently denied and removed.

---

9 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
10Working 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/
11https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2020-02-04/HL1335/
12https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras
13https://www.bbc.co.uk/news/technology-51268093
14https://www.itv.com/news/central/2019-08-16/facial-recognition-technology-allegedly-used-at-birmingham-conference-centre/

Meanwhile, the World Museum in Liverpool initially admitted to trialling the technology "following advice from Merseyside Police and local counter terrorism advisors", which both also then later denied.[15]

The Metropolitan Police and British Transport Police shared images with the Kings Cross Estate, which secretly used facial recognition surveillance encompassing one of the country's busiest national and international rail networks, and a large office and retail area.[16]

15 https://www.liverpoolecho.co.uk/news/liverpool-news/controversial-facial-recognition-used-during-16769707
16 https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c

THE ISSUES

AN UNPRECEDENTED EROSION OF CIVIL LIBERTIES

This is a turning point for facial recognition and civil liberties in the UK. If police are allowed to continue with their lawless use of facial recognition surveillance, there will be ever more uses of this authoritarian technology to track and monitor members of the public.

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, and innocent people being monitored and tracked, is the very antithesis of British notions of democratic freedom.

Big Brother Watch has successfully crowdfunded £10,000, thanks to over 280 backers, to bring a legal challenge against the Metropolitan Police and Home Office's lawless use of live facial recognition surveillance in public places.

THE THREAT TO HUMAN RIGHTS

A threat to the right to privacy

Live facial recognition surveillance 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 93% of matches inaccurately identifying innocent people.[17]

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.

17 https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-uk

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.*"[18]

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*." The Information Commissioner's Office has acknowledged that live facial recognition surveillance can *"affect large numbers of people, in many cases without their knowledge, as they go about their daily lives"* and that it can *"enable surveillance on a mass scale"* impacting *"individuals' human rights and information rights"*. [19] The Equality and Human Rights Commission has also noted that the police's use of live facial recognition may be inherently disproportionate, and has recommended that it's use should be suspended.[20]

In a challenge to police use of live facial recognition surveillance, the High Court accepted that live facial recognition surveillance does infringe people's Article 8 right to privacy.[21]

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,[22] 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.*"[23]

Proportionality is a particular concern in relation to live facial recognition surveillance 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.

> ***Case study – estimated 15m people 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.

18Biometric Commissioner, *Annual Report 2016*, September 2017, para. 305
19 ICO investigation into how the police use facial recognition technology in public places, 31st October 2019 (https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf)
20 EHRC, 'Civil and Political rights in Great Britain', March 2020 (https://www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf)
21https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf
22https://www.telegraph.co.uk/technology/2018/12/07/microsoft-president-calls-new-rules-facial-recognition-technology/
23https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

> 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".[24]

The Information Commissioner's Office has said that *"...the blanket, opportunistic and indiscriminate processing, even for short periods, of biometric data belonging to thousands of individuals in order to identify a few minor suspects or persons of interest"* [25] would not meet the high bar required by the law. However, these conditions are being completely ignored by police, who are carrying out exactly that kind of blanket, opportunistic and indiscriminate processing of biometric data belonging to thousands of people in order to identify persons of interest.

Proportionality concerns are significantly heightened in the context of the authorities' intentions. 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."*[26]

Many people have made their opposition to live facial recognition technology. Football fans have protested at several matches where live facial recognition surveillance was being used by South Wales Police. The Football Supporters Association Wales said that it treated fans like criminals, while others said that *"It feels as if our rights are being taken away".*[27]

24https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/
25https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
26South 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/)
27https://www.theguardian.com/technology/2020/jan/08/facial-recognition-at-south-wales-derby-a-step-too-far-says-police-chief

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.

> ***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.[28]

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.

Many of the people we have spoken to at trials of live facial recognition were shocked and felt both uncomfortable and targeted. Meanwhile, the London Policing Ethics Panel report on police live facial recognition surveillance found that 38% of 16-24 year-olds would stay away from events or places where facial recognition surveillance was being used, as well as high numbers of Black, Asian and Minority Ethnic people.[29]

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"*.[30]

28https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf
29 http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf
30Daily 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)

An independent review commissioned by the Metropolitan Police into their use of live facial recognition surveillance, carried out by the University of Essex, found that the legal basis for the police's use of live facial recognition surveillance was *"inadequate"*, it was *"highly possible"* it would be held unlawful if challenged in court.[31]

INNOCENT PEOPLE TARGETED

Police have used live facial recognition surveillance to target, track and monitor innocent people who aren't wanted in connection with any criminal activity.

The Metropolitan Police's 'Standard Operating Procedures' for the use of live facial recognition surveillance state that police facial recognition 'watchlists' can include people who are not wanted for a crime or who have never been arrested. Anyone deemed "of interest" to the police potentially included.[32]

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

31 https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf
32 https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mps-lfr-sop-v1-0.pdf

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.

Recent police watchlists have included thousands of people, with a deployment in central London on 27th February 2020 using a watchlist of over 7,200 people. It is not known for what purposes any of those individuals were put on the watchlist.[33]

The independent review commissioned by the Met Police stated that the police's deployments threatened "surveillance creep", with technology being used to arrest people who were not wanted by the courts, or as a justification to stop people for supposedly acting 'suspiciously' around facial recognition surveillance cameras.[34]

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.[35] A follow up study by MIT in 2019 found that Amazon's 'Rekognition' software mistook women for men 19% of the time, and darker-skinned women 31% of the time.[36] A study by the University of

33https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf
34https://www.theguardian.com/technology/2019/jul/03/police-face-calls-to-end-use-of-facial-recognition-software
35http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
36http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

Colorado also found that facial recognition technology misidentified transgender people at much higher rates.[37]

These biases can be coded into the software by programmers, albeit unintentionally, and/or due to an under-representation of black people, women and transgender people 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"*. [38]

Case study – 14-year-old black schoolchild grabbed by undercover police following facial recognition misidentification

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. The exchange was caught on film.[39]

The Metropolitan Police has admitted that its facial recognition technology evidences a significant gender bias, misidentifying women at higher rates than men.[40] Despite this, they have continued to use it operationally.

It should be noted 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.

37https://www.telegraph.co.uk/news/2019/10/30/facial-recognition-software-unable-recognise-trans-people-university/
38Biometrics and Forensics Ethics Group, Interim report, February 2019
39 https://youtu.be/gkbNH39QE0Q?t=397
40https://www.ucl.ac.uk/jill-dando-institute/events/2019/may/just-looking-learning-police-trials-live-facial-recognition; https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf

NO LAW OR LEGAL BASIS

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."[41]

> ***"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 facial recognition surveillance 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:

> "*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)."[42]

41https://www.london.gov.uk/press-releases/mayoral/independent-panel-delivers-report-on-polices-use
42Surveillance 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

Meanwhile, the Biometrics Commissioner stated that

> "*PoFA is not generic legislation covering all biometrics used by the police*" and therefore that "*the use by the police of these second generation biometrics is not currently governed by any specific legislation.*"[43]

The Biometrics Commissioner added that "*each use of biometric information the balance between public benefit and individual privacy (proportionality) should be decided by Parliament.*"[44] The Equality and Human Rights Commission said in March 2020 that the legal framework for the use of live facial recognition is insufficient, and that is use should be suspended.[45]

Despite this, the government has allowed the police to act in this lawless space. 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.*" [46]

Live facial recognition surveillance is a rights-altering technology that will significantly erode privacy and civil liberties in the UK. We believe that it is incompatible with the Human Rights Act and that proper parliamentary consideration is urgently required – particularly given the technology's significant and unique impact on rights in the UK.

NO POLICY

Live facial recognition surveillance is fundamentally incompatible with the right to privacy and freedom of expression, on our analysis; a view shared by the independent reviewers of the Met Police's technology.[47] 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: how are people put on police watchlists, which databases can be matched against, which images

43Biometrics Commissioner, Annual Report 2017 (June 2018)
44Biometrics Commissioner, Annual Report 2017 (June 2018)
45 EHRC, 'Civil and Political rights in Great Britain', March 2020 (https://www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf)
46Letter from Baroness Williams, Minister for the Home Office, to the Chair of the Science and Technology Committee, 30 November 2017 ()
47https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

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"* .[48]

There is also no policy limiting the purposes for which live facial recognition surveillance can be used.

Biometrics Strategy

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 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]."*[49]

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.[50] 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.

48Written 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
49Home Office Biometrics Strategy (June 2018)
50Home Office Biometrics Strategy (June 2018)

NO EFFECTIVE OVERSIGHT

Police have said they will seek oversight of their use of live facial recognition surveillance 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: "*Clarity regarding regulatory responsibility is an emerging issue, for example in automatic facial recognition use by police – which regulator has responsibility*"[51] and has said that the Government "*appears to leave oversight and management of this process solely to the police*".[52] The Commissioner said he hoped the the Biometric Strategy would "*provide 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.

The Biometrics Commissioner has said that the trials required "*independent oversight to reassure the public*",[53] and that "*deciding what is proportionate should not be left to those who seek to benefit from the use of the biometric.*"[54]

The Information Commissioner's Office has said that

> *"there is a balance to be struck between the privacy that people rightly expect when going about their daily lives and the surveillance technology that the police need to effectively carry out their role."* [55]

However, its clear that that balance is not being struck by police, nor could the indiscriminate processing of thousands of people's biometrics just to find a few people on a police watchlist could ever strike that balance.

A new Law Enforcement Facial Images and Biometrics Oversight and Advisory Board began in 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.

---

51 Review of the impact and operation of the Surveillance Camera Code of Practice –Surveillance Camera Commissioner, Feb 2016, p.15
52 Surveillance Camera Commissioner, Annual Report 2016/17 (January 2018)
53https://www.gov.uk/government/news/metropolitan-polices-use-of-facial-recognition-technology-at-the-notting-hill-carnival-2017
54Biometrics Commissioner, Annual Report 2017 (June 2018)
55https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

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*."[56]

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*."[57]

This lack of meaningful oversight has resulted in some extremely concerning uses of live facial recognition surveillance, as previously noted, including the targeting of peaceful protestors, innocent people with mental health problems, and tens of thousands of innocent members of the public at shopping centres, high streets, football matches, music concerts and transport hubs.[58]

56Information 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
57http://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
58https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-map

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.

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 police themselves in response to Freedom of Information requests.

- **NEW:** In its entire four years of deployments since 2016, the Metropolitan Police's live facial recognition surveillance has been **93% inaccurate.**[59] In two of the three deployments in 2020, the Met Police had a **100% failure rate** - not identifying a single person.[60]
- **NEW:** At the most recent deployment in central London in February 2020, the Met Police **intervened in 71% of misidentifications, stopping innocent people**, which can result in misidentified people being asked for identification, sometimes searched and even fingerprinted.[61] This shows a **clear presumption to intervene**, despite the high rate of misidentifications.
- **NEW:** Overall since June 2017, South Wales Police have used live facial recognition surveillance 70 times, with **88% of its matches being inaccurate.**[62]
- **NEW:** At **27 of 70 deployments,** South Wales Police **didn't have a single positive identification**, and at **39 of them**, they **didn't make a single arrest.**
- This already evidences arbitrary policing; but used on a mass scale, the error rate would be untenable.

The independent review commissioned by the Metropolitan Police also found that the police's facial recognition surveillance was significantly inaccurate. Their analysis looked only at 6 of the police's trials, and found that the Met's facial recognition technology was accurate only 19% of the time – inaccurate 81% of the time.[63]

59 https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-map
60https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf
61https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf
62 http://afr.south-wales.police.uk/
63https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

OVER-POLICING: CASE STUDIES

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 – innocent man stopped by police for covering face, fined

A middle aged white 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 surrounded him, demanded his ID, and the man complied. However, as he was protesting angrily at being stopped for no good reason, 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. The incident was caught on camera by the BBC.[64]

Case study 2 – innocent young man stopped for covering his face with scarf

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.

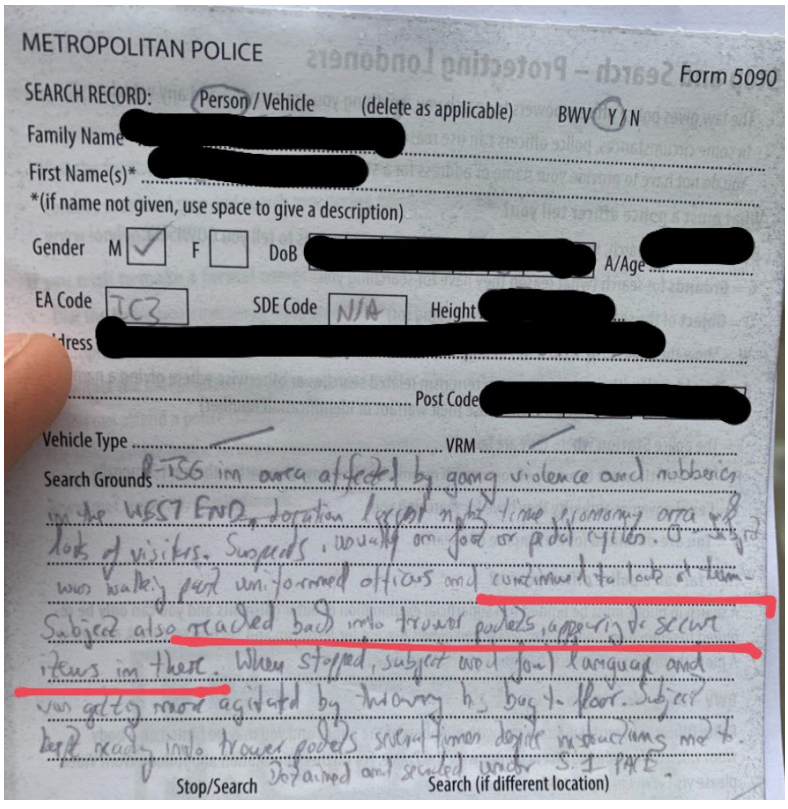
64https://www.youtube.com/watch?v=0oJqJkfTdAg

Case study 3 – young boy in school uniform wearing a hoodie stopped and asked for identification

On the coldest day of the year in 2019, a young black child 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.

Case study 4 – innocent young men stopped and searched in vicinity of cameras

We have observed further aggressive stop and search tactics carried out by officers on duty at facial recognition deployments, racially profiling numerous young black men as 'acting suspiciously' in the vicinity of the live facial recognition surveillance cameras. One man was stopped for "looking at officers" and "reaching into his trouser pockets", while another was told it was "suspicious" he was walking slowly.[65] The stop and search receipt provided by the police is below.


METROPOLITAN POLICE

Form 5090

SEARCH RECORD: (Person) / Vehicle (delete as applicable) BWV (Y) / N

Family Name [redacted]

First Name(s)* [redacted]

*(if name not given, use space to give a description)

Gender M ✓ F ☐ DoB [redacted] A/Age [redacted]

EA Code IC3 SDE Code N/A Height [redacted]

Address [redacted]

Post Code [redacted]

Vehicle Type ..... VRM .....

Search Grounds R-ISG in area affected by gang violence and robberies in the WEST END, location target night time crime area full of visitors. Suspects usually on foot or pedal cycles. Officers was walking past uniformed officers and continued to look at them. Subject also crammed hand into trouser pockets, appearing to secure items in there. When stopped, subject used foul language and was getting more agitated by having his bag to floor. Subject kept ready into trouser pockets several times despite instructions not to. Obtained and searched under S.1 PACE.

Stop/Search Search (if different location)

65https://www.independent.co.uk/news/uk/crime/stop-search-london-met-police-black-man-hands-pockets-oxford-circus-a9349311.html

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.[66]

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.[67] In February 2020, the European Court of Human Rights ruled that even convicted people's photos and biometric data cannot be stored indefinitely.[68]

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 surveillance. 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.

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* ***for the retention of DNA samples and fingerprints should also be applied to the retention of custody images"***[69]

The Biometrics Commissioner has said that at the time of Custody Image Review *"I was not at all sure this would meet further court challenges. I still think that."*[70] The Commissioner said in March 2019 that *"I am not sure that the legal case is strong enough and that it would withstand a further court challenge."* [71]

66 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
67 *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)
68 *Gaughran v the United Kingdom* (Application No. 45245/15) [2020] (http://hudoc.echr.coe.int/eng?i=001-200817)
69 Annual Report – Biometrics and Forensics Ethics Group, October 2017, pg. 9
70 https://parliamentlive.tv/Event/Index/f9d3913e-b5c2-41e6-8452-de80f49e85e9
71 https://parliamentlive.tv/Event/Index/f9d3913e-b5c2-41e6-8452-de80f49e85e9

OPPOSITION

Cross-party support & 26 human rights groups

In September 2019, 26 rights, race equality and technology groups, as well as cross-party MPs including David Davis MP, Diane Abbott MP, Ed Davey MP, and Caroline Lucas MP, called for an "immediate stop" to facial recognition surveillance.[72] They also raised 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.

The organisations included Big Brother Watch, Amnesty International, Ada Lovelace Institute, Article 19, Liberty, the Institute of Race Relations, Race Equality Foundation, Runnymede Trust, Race on the Agenda, Index on Censorship, the Police Action Lawyers Group, Netpol, The Joint Council for the Welfare of Immigrants, Open Rights Group, The Monitoring Group, Tottenham Rights, and the Football Supporters Association.[73]

Equality and Human Rights Commission

The Equality and Human Rights Commission has said live facial recognition surveillance should be suspended as the legal framework is insufficient, it may be inherently disproportionate, and it may operate in a discriminatory manner.[74]

Science and Technology Committee

The Science and Technology Committee has called for a moratorium on the police's use of the technology.[75]

Scottish Parliament

The Scottish Parliament stated in February 2020 that there was "no justification" for police to use live facial recognition surveillance, and that it would be a "radical departure" from policing by consent, following an inquiry into Police Scotland's proposed use of facial recognition surveillance. [76]

Police and Crime Commissioners

72https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019.pdf
73https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf
74 EHRC, 'Civil and Political rights in Great Britain', March 2020 (https://www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf)
75 https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf
76https://www.bbc.co.uk/news/uk-scotland-51449166

Police and Crime Commissioners have voiced their concern about police use of live facial recognition surveillance. The North Wales Police and Crime Commissioner has said that *"It is invasive, disproportionate and has the ability to reduce confidence in our policing,"*, while the Dyfed Powys Police and Crime Commissioner has said that it *"over steps the mark".* [77]

Legal challenge

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 surveillance had infringed people's Article 8 right to privacy and Article 10 rights to freedom of expression and association.[78] In light of the recent decision by the Metropolitan Police to operationally deploy live facial recognition surveillance across London, we are urgently considered our next steps.

CONCLUSION

We urge parliamentarians 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.**

77 https://twitter.com/DafyddLlywelyn/status/1188412133475782658
78 https://www.crowdjustice.com/case/face-off/