

**LIBERTY**

**BIG  
BROTHER  
WATCH**

**LIBERTY AND BIG BROTHER  
WATCH'S RESPONSE TO THE  
SURVEILLANCE CAMERA CODE  
OF PRACTICE CONSULTATION**

**SEPTEMBER 2021**

## **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 that we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

## **ABOUT LIBERTY**

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at [libertyhumanrights.org.uk/policy](https://libertyhumanrights.org.uk/policy).

# **CONTACT**

## **SILKIE CARLO**

Director

[silkie.carlo@bigbrotherwatch.org.uk](mailto:silkie.carlo@bigbrotherwatch.org.uk)

## **MARK JOHNSON**

Legal and Policy Officer

[mark.johnson@bigbrotherwatch.org.uk](mailto:mark.johnson@bigbrotherwatch.org.uk)

## **EMMANUELLE ANDREWS**

Policy and Campaigns Officer

[emmanuelle.a@libertyhumanrights.org.uk](mailto:emmanuelle.a@libertyhumanrights.org.uk)

# INTRODUCTION

The Government is consulting on changes to the surveillance camera code of practice, which was introduced under section 30 of the Protection of Freedoms Act 2012. Updates to the code are intended to reflect some changes to legislation and the judgment in *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 ('Bridges'), where the use of live facial recognition technology by the force in question was found to have been unlawful.

Facial recognition is invasive, inaccurate and discriminatory. We do not believe that it has a place in a rights-respecting democracy. As such, we reject the notion that the Surveillance Camera Code of Practice could constitute a legitimate framework for the police's use of live facial recognition in the UK. It is our view that the novel rights impact of live facial recognition technology makes its public use a matter for urgent parliamentary consideration. In particular, we believe Parliament should ban the police's use of live facial recognition altogether.

## **THE SURVEILLANCE CAMERA CODE OF PRACTICE IS NOT A SUITABLE FRAMEWORK FOR THE USE OF LIVE FACIAL RECOGNITION IN THE UK**

There remains no explicit legal basis for the use of live facial recognition by police forces in the UK.

The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras in England and Wales. As a result, the Surveillance Camera Code of Practice was issued by the Secretary of State in 2013 under section 30 of the Act. However, there is no reference to facial recognition in the Act itself or indeed in any other UK statute.

Neither House of Parliament has ever considered or scrutinised automated facial recognition technology. A lack of adequate parliamentary scrutiny before the adoption of a new technology that significantly interferes with individuals' rights is entirely unacceptable.

This lack of a clear statutory footing for facial recognition was something the previous Surveillance Camera Commissioner himself raised.<sup>1</sup>

---

<sup>1</sup> [A National Surveillance Camera Strategy for England and Wales](#) – Surveillance Camera Commissioner, March 2017, para. 35, p.12

Amendments to the Code which follow Bridges could be read as legitimising the use of this technology, despite the fact it has not been subject to democratic oversight.

Factoring in the proposed amendments, there are but four passing references to facial recognition in the Code itself. This scant guidance cannot be considered a suitable regulatory framework for the use of facial recognition, indeed nor could any other legislation or guidance relevant to facial recognition technology – such as the recently drafted College of Policing Guidance<sup>2</sup> – provide an adequate legal framework that would either satisfy the deficiencies of the amended Surveillance Camera Code in providing the safeguards required by Bridges nor protect the clear human rights abuses the tech presents.

## **WE NEED A FULL NATIONAL SURVEILLANCE CAMERA REVIEW IN THE UK**

Surveillance in the UK is excessive, invasive and oppressive. The UK is now the most camera-surveilled country in the Western World. According to recently published statistics, London remains the third most surveilled city in the world, with 73 surveillance cameras for every thousand people.<sup>3</sup>

Many surveillance cameras in the UK now have advanced capabilities such as biometric identification, behavioural analysis, anomaly detection, item/clothing recognition, vehicle recognition and profiling. Surveillance cameras are no longer only passively recording but are often actively analysing public spaces and the individuals within them. A review is needed to investigate the novel rights impacts of these technologies, the scale of surveillance we live under, and the regulations and interventions needed to prevent the country from becoming a dystopian surveillance state.

The slow and silent deployment of facial recognition surveillance in the UK is a dangerous next step. Rather than update toothless codes of practice to legitimise the use of new technologies like live facial recognition, the UK should have a root and branch surveillance camera review which seeks to increase accountability and protect fundamental rights.

---

<sup>2</sup> See here for Big Brother Watch and Liberty's open letter with 29 other NGOs in response to the College of Policing's draft guidance: <https://privacyinternational.org/advocacy/4583/pi-and-allies-respond-college-policing-consultation-stating-live-facial-recognition>

<sup>3</sup> The Most Surveilled Cities in the World, Statista, 23 August 2021, <https://www.statista.com/chart/19256/the-most-surveilled-cities-in-the-world/>

## **PARLIAMENT MUST BAN THE POLICE'S USE OF LIVE FACIAL RECOGNITION**

Facial recognition cameras perform instantaneous biometric identity checks without the consent of those they surveil. The technology inverts the vital democratic principle of suspicion preceding surveillance, treating members of the public like suspects. This has the effect of turning us into walking ID cards subject to high-tech police line ups and is a direct threat to the right to privacy.

Despite its highly invasive nature, live facial recognition does not make populations safer as its proponents argue. The technology is highly inaccurate and during their trial of live facial recognition between 2016-19, Big Brother Watch research found that the Metropolitan Police had an inaccuracy rate of 93% in confirming face “matches”.

Live facial recognition is also inherently discriminatory and poses a direct threat to minority communities. The Court of Appeal in *Bridges* noted that there is scientific evidence that facial recognition can be biased and create a greater risk of false identifications in these cases. Similarly, a study conducted by the Massachusetts Institute of Technology into the commercial use of artificial intelligence systems found that the error rate of facial recognition software was 43 times higher for dark-skinned women than it was for light-skinned men,<sup>4</sup> and when exercising their rights under Articles 8, 10 and 11, members of these groups are likely to be treated less favourably than others in the same position by virtue of their sex or race, including through being more likely to be wrongly stopped and questioned by police, and to have their images retained as the result of a false match. Research has also shown how trans and non-binary people are regularly misidentified by the tech, leading these communities vulnerable to situations of embarrassment, and contributing to stigmatisation.<sup>5</sup> And finally, studies have highlighted the disproportionate misidentification of disabled people by facial recognition technology.<sup>6</sup>

Liberty and Big Brother Watch do not believe that these failings can ever be mitigated, and it is clear that the Surveillance Camera Code of Practice is an entirely unsuitable framework to address the serious rights risk posed by the use of live

---

<sup>4</sup> Buolamwini, Joy; Geburu, Timmit: *Gender Shades – Intersectional Accuracy Disparities in Commercial Gender Classification*. In: *Proceedings of Machine Learning Research* 81:1, p.1-15, 2018. Available from <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>, p.1.

<sup>5</sup> Privacy International (2021), *Threats in the usage of facial recognition technologies for authenticating transgender identities*. Available at: <https://privacyinternational.org/news-analysis/4474/threats-usage-facial-recognition-technologies-authenticating-transgender>

<sup>6</sup> Sheri Byrne-Haber (2019), *Disability and AI Bias*. Available at: <https://sheriyrnehaber.medium.com/disability-and-ai-bias-cced271bd533>

facial recognition in public spaces in the UK. This technology is inherently discriminatory and incompatible with a rights-respecting democracy like the UK. Moreover, as a police surveillance tool, we are concerned that deployments of this surveillance technology would mirror and exacerbate existing disproportionate policing practices (such as stop and search and the Gangs Matrix) in being most frequently used to monitor people of colour and those on lower incomes. The racial and socio-economic dimensions of police trial deployments are instructive in this regard.<sup>7</sup>

Liberty and Big Brother Watch believe that only a total ban on the use facial recognition technology for public surveillance would ensure that our rights are protected.

---

<sup>7</sup> For example, the Met has deployed facial recognition at Notting Hill Carnival for two years running, a festival celebrating Black Caribbean culture in the UK, as well as twice in the London Borough of Newham. Newham is one of the UK's most ethnically diverse places and the white British population stands at 16.7%, the lowest in the UK.