LIBERTY

LIBERTY'S BRIEFING ON THE AMENDED SURVEILLANCE CAMERA CODE OF PRACTICE

JANUARY 2022

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.

CONTACT

SAM GRANT

Head of Policy and Campaigns

samg@libertyhumanrights.org.uk

EMMANUELLE ANDREWS

Policy and Campaigns Manager

emmanuellea@libertyhumanrights.org.uk

JUN PANG

Policy and Campaigns Officer

junp@libertyhumanrights.org.uk

INTRODUCTION

1. The Government has laid an amended Surveillance Camera Code of Practice (COP) before Parliament pursuant to section 31(3) of the Protection of Freedoms Act 2012. The amended COP is a result of a public consultation between 13 August 2021 and 8 September 2021. 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 was found to have been unlawful.

2. Notwithstanding the amendments made to the COP, we maintain that 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. Indeed, the Court of Appeal in Bridges held that the Surveillance Camera Code of Practice 2013 did not satisfy the human rights requirement of being 'in accordance with the law.' It is our view that the novel rights impact of live facial recognition technology make its public use a matter for urgent parliamentary scrutiny. **For the unmitigable rights violations posed by facial recognition technology, we urge parliamentarians to vote against the amended COP, and move to ban the use of LFR and facial recognition technology more broadly.**

HOW DOES FACIAL RECOGNITION TECHNOLOGY WORK

3. In brief, live facial recognition[1] cameras scan the distinct facial points of every passer-by and create a unique biometric map in the form of a numerical code. This code is matched against corresponding codes from faces on police watch lists. It is being deployed at sporting events, concerts and festivals, in city centres, on busy shopping streets, as part of everyday police operations – and even at protests.[2] More recently, facial recognition technology has been used

[1] Police forces may refer to live facial recognition as "AFR Locate", to distinguish it from non-live facial recognition programs used to match still photographs to a watch list ("AFR Identify"). All references to facial recognition in this briefing refer to the use of facial recognition in live settings, unless otherwise stated.

[2] South Wales Police list their deployments of facial recognition online (see: http://afr.south-wales.police.uk/#deployments). The Met have deployed facial recognition on ten occasions Notting Hill Carnival in 2016 and 2017, Remembrance Day 2017, Port of Hull docks (in partnership with Humberside Police) in 2018, Stratford transport hub for two days in June and July 2018, Central London in December 2018 and Romford for two days in January and February 2019. Leicestershire police deployed facial recognition at Download Music Festival in 2015 (see: https://www.independent.co.uk/news/uk/crime/download-festival-facial-recognition-technology-used-at-event-could-be-coming-to-festivals-10316922.html).

in supermarkets.[3] In October, it was reported that nine schools in North Ayrshire had begun deploying facial recognition technology as a way for pupils to buy their lunch, although swift interventions by civil society groups, parliamentarians, and eventually the Information Commissioner's Office forced a u-turn.[4] In December, South Wales Police – the police force subject to challenge in *Bridges* – announced that it is developing the first mobile app for facial recognition in policing in the UK.[5]

4. Apart from LFR technology, we are also aware of the use of retrospective facial recognition (RFR), which compares an image of an individual against a database of custody images. The images can be taken from a variety of different recorded footage, such as CCTV footage and footage from social media. The Metropolitan Police has previously explained that it has begun to use near "real-time searching" or "LFR Operator initiated searching using mobile devices" where an officer takes a picture of a subject and submits it for immediate search.[6] The Home Office explains that the recorded footage is compared against the Police National Database (PND), which contains millions of images of police suspects.[7] The Royal Society of Arts (RSA) has found that all territorial police forces have access to RFR through the PND, noting its concern about the "relative unwillingness of forces to detail their use of retrospective facial recognition through the freedom of information process".[8]

THERE IS NO LEGAL BASIS FOR THE USE OF LIVE FACIAL RECOGNITION BY POLICE FORCES IN THE UK

5. In spite of the use of facial recognition technology across many areas of society – and proposals to extend this even further – there has not been proper democratic scrutiny over its application.

---

[3] Chivers, T., *Facial recognition... coming to a supermarket near you,* The Guardian, 4 August 2019, available at: https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties

[4] BBC News, *Schools pause facial recognition lunch plans,* 25 October 2021, available at: https://www.bbc.co.uk/news/technology-59037346

[5] https://twitter.com/swpolice/status/1468582046591160321?ref_src=twsrc%5Etfw

[6] See: https://twitter.com/MetPoliceEvents/status/1431212920252289027; https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mpf-lfr-guidance-document-v1-0.pdf and https://inews.co.uk/news/technology/uk-police-testing-retrospective-facial-recognition-identify-criminals-1128711

[7] Home Office, *Fact Sheet on live facial recognition used by police,* 4 September 2019, available at: https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/

[8] Grimond, W. and Singh, A., *A Force for Good? Results from FOI requests on artificial intelligence in the police force*, April 2020, available at: https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf

6. **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.

7. The amended COP is intended as an update to the 2013 document. Factoring in the proposed amendments, however, 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. In our view, no other legislation or guidance relevant to facial recognition technology – such as the recently drafted College of Policing Guidance[9] – could furnish an adequate legal framework to mitigate for the deficiencies of the amended Surveillance Camera Code, provide the full safeguards required by Bridges, or address the clear human rights abuses this technology presents.

8. **Crucially, neither House of Parliament has ever adequately considered or rigorously scrutinised automated facial recognition technology.** A lack of adequate parliamentary scrutiny before the adoption of a new technology that significantly interferes with individuals' fundamental rights is entirely unacceptable. This lack of a clear statutory footing for facial recognition was something the previous Surveillance Camera Commissioner himself raised.[10]

9. In particular, we are highly concerned by the following threats posed by facial recognition technology to our fundamental rights:
    - **A fundamental threat to our privacy, dignity, and autonomy:** Being able to choose when and how to disclose one's identity, and to whom, is at the heart of a person's dignity and autonomy. In some cases, identification determines how the State interacts with people and whether they are afforded access to their rights. The use of facial recognition – which affects everyone who passes by the camera - therefore represents a huge shift in the relationship between the

[9] 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

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

individual and the State, and for our right to remain anonymous more broadly. The recent example of the deployment of facial recognition technology in schools raises further questions about the disproportionate ways that FRT can impact on specific groups, including children.[11]

- **A threat to our rights to freedom of expression and freedom of association:** The use of facial recognition technology can be highly intimidating. If we know our faces are being scanned by police and that we are being monitored when using public spaces, we are more likely to change our behaviour.[12] Those changes in behaviour may relate to where we go and who we choose to associate with. For a whole host of reasons linked to a desire to retain our anonymity and to keep our activities and political views private, we may decide not to attend public meetings, to avoid our local high street, or change who we spend time with in public spaces. For example, Liberty has worked with protesters who expressed how intimidating they found the presence of facial recognition at demonstrations, and who said that they would be reluctant to attend a future protest where it was in use. Forty per cent of people aged 16-24 said they simply would not attend an event where facial recognition was being deployed.[13]

- **A threat to our democracy:** The UK has a shameful history of subjecting political activists to invasive state surveillance. The European Court of Human Rights recently held that the UK had violated the right to privacy of Mr John Catt, a peace movement activist who – despite having never being convicted of any offence – had his name and other personal data included in a police database and was subject to intrusive surveillance.[14] In entrenching and exacerbating this pattern, the expansion of facial recognition technology will undermine our ability to express ideas and opinions, communicate with others

[11] See Lord Scriven, HL Deb 4 November 2021, vol. 851, col. 1400: "This debate is not about technology; it is about the use of a child in terms of the autonomy of that child's body."
[12] Studies have shown that people were less inclined to attend mosques they thought were under government surveillance. Business owners muted political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook. See: Shamas et al (2103), *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Muslim American Civil Liberties Coalition (MACLC), and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, available at: http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf
[13] London Policing Ethics Panel, *Final Report on Live Facial Recognition*, 2019, available here: http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lfr_final_report_-_may_2019.pdf
[14] *Catt v United Kingdom* 43514/15, [2019] ECHR 76

and engage in democratic processes, as people increasingly choose not to pay the price of handing over their sensitive biometric data in order to do so.

- **Discriminatory and inaccurate:** A range of studies has shown that facial recognition technology disproportionately misidentifies women and BAME people[15][16] – meaning that people from these groups are more likely to be wrongly stopped and questioned by police, and to have their images retained as the result of a false match. In *Bridges,* the Court of Appeal noted that there is scientific evidence that facial recognition can be biased and create a greater risk of false identifications in the case of women and BAME people. 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. In addition, research has also demonstrated how trans and non-binary people are regularly misidentified by this technology, leading these communities to be vulnerable to situations of embarrassment, and contributing to stigmatisation.[17] Studies also show the disproportionate misidentification of disabled people by facial recognition technology, and AI more broadly.[18] We are highly concerned that police use of facial recognition in particular is likely to mirror existing disproportionate policing practices (i.e. stop and search,[19] the Gangs Matrix[20]) 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.[21] Contrary to the Surveillance Camera Code of Practice's assurances, it is both the ways in which

[15] Buolamwini et al (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 2018 Conference on Fairness, Accountability, and Transparency

[16] Klare et al (2012), *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security, Available at: https://ieeexplore.ieee.org/document/6327355.

[17] 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

[18] Sheri Byrne-Haber (2019), *Disability and AI Bias. Available at: https://sheribyrnehaber.medium.com/disability-and-ai-bias-cced271bd533*

[19] Official figures show people who identify as black in England and Wales are nearly 10 times more likely to be stopped than people who identify as white. See: GOV.UK Ethnicity Facts and Figures, *Stop and Search,* 19 March 2020, Available at: https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest

[20] The Gangs Matrix was part of a highly- politicised response to the 2011 London riots. More than three- quarters (78 per cent) of the 'gang nominals' included on the database are black, a disproportionate number given the Met's own figures show that only 27 per cent of those responsible for serious youth violence are black. See: Wiilliams (2018), *Being Matrixed: The (over)policing of gang suspects in London,* StopWatch, Available at: https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

[21] 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.

surveillance camera technology is used *and* the technology itself that renders it so intrusive. [22] For the ways in which facial recognition technology exists to be used in discriminatory institutions, as well as the way in which the tech itself compounds the discrimination experienced by those from marginalised communities, we do not believe facial recognition technology can ever be debiased.

PARLIAMENT MUST VOTE DOWN THE CODE OF PRACTICE AND BAN THE USE OF FACIAL RECOGNITION TECHNOLOGY

10. 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.[23] 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.

11. Simultaneously, the breadth of public concern around this issue is growing clearer by the day. At the time of writing, Liberty's petition calling for a ban against the use of facial recognition in publicly accessible places has over 65,000 signatories,[24] 31 national and international civil society organisations have published an open letter calling for facial recognition technology by police and private companies to be banned, [25] and a statement released in September 2019 by Big Brother Watch was signed by politicians from across the political spectrum and 25 race equality and technology campaign groups – as well as technology academics and legal experts.[26] Several cities in the US have banned the use of facial recognition,[27] and the European

[22] Draft Surveillance Camera Code of Practice, p.5
[23] The Most Surveilled Cities in the World, Statista, 23 August 2021, https://www.statista.com/chart/19256/the-most-surveilled-cities-in-the-world/
[24] See: https://liberty.e-activist.com/page/46698/petition/1
[25] *Civil Society Groups: Live Facial Recognition Technology should not be used in public spaces*, Privacy International, August 2021, available at: https://privacyinternational.org/sites/default/files/2021-08/LFRT%20Open%20Letter%20Final.pdf
[26] Big Brother Watch, *Joint statement on police and private company use of facial recognition surveillance in the UK*, 2019, available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf
[27] Conger, K., Fausset, R., and Kovaleski, S.F., *San Francisco Bans Facial Recognition Technology,* The New York Times, 14 May 2019, available at: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; Ravani, S., *Oakland bans use of facial recognition technology, citing bias concerns*, San Francisco Chronicle, 16 July 2019, available at:

Parliament has called for a ban on police use of facial recognition technology in public places and predictive policing.[28] In response to the Black Lives Matter uprisings in 2020, Microsoft, IBM, and Amazon announced that they would cease selling facial recognition technology to US law enforcement bodies.[29] Facebook also recently announced that it will be shutting down its facial recognition system and deleting the "faceprints" of more than a billion people after concerns were raised about the technology.[30]

12. Liberty does not believe that the above identified rights risks 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 facial recognition in public spaces in the UK. We echo the concern voiced by Lord Clement-Jones in a recent debate on facial recognition technology in schools that the expansion of such tools is "a short cut to a widespread surveillance state."[31] 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. The review should investigate the novel rights impacts of these technologies, the scale of surveillance we live under, and the regulations and interventions needed to uphold our rights.

13. Furthermore, Liberty believes that only a total ban on the use facial recognition technology for public surveillance would ensure that our rights are protected. **We urge parliamentarians to vote against the amended COP, and move to ban the use of LFR and facial recognition technology more broadly.**

https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; Jarmanning, A., *Boston Bans Use Of Facial Recognition Technology. It's The 2nd-Largest City To Do So*, WBUR, 24 June 2020, available at: https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban

[28] Hekkila, M., *European Parliament calls for a ban on facial recognition,* 6 October 2021, available at: https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/

[29] Magid, L,. *IBM, Microsoft and Amazon not letting police use their facial recognition technology,* Forbes, 12 June 2020, available at: https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/

[30] Milmo, D., Facebook to shut facial recognition system and delete 1bn 'faceprints', 2 November 2021, available at: https://www.theguardian.com/technology/2021/nov/02/facebook-to-shut-facial-recognition-system-and-delete-1bn-faceprints

[31] Lord Clement-Jones, HC Deb 4 November 2021, vol.815, col. 1395.