Big Brother Watch evidence to the Justice and Home Affairs Committee inquiry on live facial recognition

2. What is the legal basis for the use of Live Facial Recognition technology by police forces in England and Wales?

There is no legislative basis that creates the police powers for the use of LFR. There is no primary or secondary legislation which mentions facial recognition, and the technology has never been debated in the House of Commons. The most detailed parliamentary examination of LFR, undertaken by the Science and Technology Committee in 2019, called for a stop to its use, citing concerns over the lack of legal framework.[1]

The Metropolitan Police Service (MPS) and South Wales Police (SWP) have stated that common law policing powers are a sufficient basis for their deployment of LFR, citing the Court of Appeal judgment in *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 (*Bridges).* This judgment assessed SWP's deployments of LFR in Cardiff in 2017 and 2018 and found it had been unlawful, but that common law policing powers could be relied on by police when deploying LFR. However, it is important to note that the Court stated that its judgment did not give police forces a green light to proceed with this technology, and instead should be read as an assessment of the facts specific to the *Bridges* case: "Whether other uses of police power in other contexts will be lawful in the future will be a matter to be considered if the facts of such a case arise in practice."[2] The Court also noted that there were "fundamental deficiencies" in the legal framework currently in place.[3] Police use of LFR has progressed significantly since 2017 and is used more frequently, with much larger watchlists.

Police forces have also made reference to multiple pieces of legislation such as the Data Protection Act 2018, the Human Rights Act 1998 and the Equality Act 2010 as providing the legal justification for their use of LFR. As Baroness Chakrabarti noted in the Committee's oral evidence session, these pieces of legislation "do not create police powers of any kind; they constrain them".[4] They cannot be considered a lawful basis for the deployment of LFR. The Ryder Review, an independent legal review of the governance of biometric data in England and Wales, has argued that using existing sources of law "as the entry point for biometric governance, fails to take into account some of the specific features and specific risks posed by biometrics, particularly on the group level."[5]

Both SWP and the MPS have cited the Surveillance Camera Code of Practice (the SCCoP) and the College of Policing's Authorised Professional Practice on LFR (the APP) as providing a legal framework for police use of LFR. These instruments are addressed in response to Q5, but it should be noted that neither the SCCoP or the APP are legally binding or enforceable.

It remains that neither the public nor Parliament has had a say in the use of this incredibly powerful new form of surveillance. The lack of democratic mandate for LFR is deeply concerning. The UK is increasingly an outlier in the democratic world in taking this approach, with European countries, the EU, US states and cities banning or severely restricting law enforcement use of LFR.

4. Has there been sufficient research and advice, readily available to police forces, to enable them to make informed decisions about the acquisition of LFR?

There is no lack of research or advice on LFR available to police forces. A parliamentary committee, multiple Biometric and Surveillance Camera Commissioners, academic studies, reports from rights groups and international bodies such as the UN and EU have documented in detail the legal, ethical and operational risks of law enforcement agencies deploying LFR. Both SWP and the MPS have chosen not to follow the recommendations of human rights and technology experts around the world.[6]

The MPS, for example, commissioned a report from the University of Essex into its use of LFR. The 2019 report, which won a Celebrating Excellence in Research and Impact Award for

1 The work of the Biometrics Commissioner and the Forensic Science Regulator – Science and Technology Committee, Nineteenth Report of Session 2017–19, 17th July 2019, HC 1970: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf

2 Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058 (11 August 2020), para 60

3 Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058 (11 August 2020), para 91

4 Uncorrected oral evidence: Live facial recognition – Justice and Home Affairs Committee, 12th December 2023: https://committees.parliament.uk/oralevidence/14009/pdf/

5 Independent legal review of the governance of biometric data in England and Wales – Matthew Ryder KC, Ada Lovelace Institute, June 2022: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

6 See for example: Over 180 rights groups and tech experts call for global stop to facial recognition surveillance – Big Brother Watch, 26th September 2023: https://bigbrotherwatch.org.uk/2023/09/180-tech-experts-call-for-global-stop-to-facial-recognition-surveillance/

Outstanding Interdisciplinary Research, found "significant operational shortcomings" in the the MPS' use of LFR and "called for all live trials of LFR to be ceased" due to human rights concerns.[7] The MPS has not acknowledged the report's findings and has not made it available on its website. Instead, the force proceeded to expand its use of LFR.

5. Is there written guidance available to those operating LFR, and, if it exists, what does that guidance contain?

As noted above, both the MPS and SWP have referenced the APP and SCCoP as part of the "complex patchwork" that provides the legal basis for the deployment of LFR by police forces.[8] This complex patchwork does not consist of any legally binding guidance and has largely been authored by police forces themselves. The Ryder Review notes: "In the absence of a clearer oversight structure, the numerous codes of practice or guidance notes issued by different public authorities at various times create confusion, rather than clarity."[9]

The SCCoP was introduced by the Protection of Freedoms Act 2012, and provides guidance on the appropriate use of surveillance camera systems by relevant authorities. Authorities must "have regard" to the Code, but it is not legally enforceable. It did not initially contain any references to LFR, but was updated in 2021 to reflect the judgment in *Bridges*, where the use of LFR was found to have been unlawful. There are just four passing references to facial recognition in the SCCoP itself. This scant guidance cannot be considered a suitable regulatory framework for the use of facial recognition. Additionally, the SCCoP is due to be abolished, along with the post of the Biometrics and Surveillance Camera Commissioner, who is responsible for overseeing the SCCoP, via the Data Protection and Digital Information Bill.

Lindsey Chiswick, Director of Intelligence at the MPS, stated during the Committee's evidence session that the legal basis for LFR is "underpinned now by the [APP] from the College of Policing".[10] The guidance, being authored by police itself, is highly enabling and sets out a broad series of uses for LFR. Rather than just being used to locate those wanted for criminal offences, it also suggests LFR should be used for preventing people who "may cause harm" from entering an area, locating people about whom there is intelligence to suggest that they "may pose a risk of harm to themselves or others". This vague category of 'preventing harm' could be used by police forces to justify almost any kind of use. Indeed the guidance notes that preventing "financial harm, including (...) dishonesty" could be a use case for LFR – not financial *crime*.[11] Of serious concern is the expansive categories of individuals that the guidance suggests can be placed on a LFR watchlist. As well as those wanted for criminal offences, watchlists can include a broad range of individuals, many of whom have committed no criminal offence and are not suspected of doing so. The categories can include a victim of an offence, a witness to a crime or a close associate of any category of individual that can be placed on a watchlist. Targeting "associates" of suspects, particularly of low grade crime, associates of those who might pose the 'risk of harm', possible witnesses and even victims of crimes is an enormous expansion of policing surveillance tools. However, because individuals are not informed if they have been added to police facial recognition watchlists, there is no way to test the necessity and proportionality of the composition of the watchlists.

The guidance states that as well as the database of 19 million custody images (many of which will be of innocent people), forces can use "police originated non-custody images" and "non-police originated images". The latter can provided by and/or sourced from public bodies, law enforcement partners (including those outside the UK), private companies and/or individuals. This extraordinarily broad policy gives police forces total discretion as to where they source images from, and opens the door to practices like social media scraping, where private companies harvest the images of millions of innocent people and sell these images to police forces.[12] Ministers have already announced plans to use the passport database and driving licence database for facial recognition searches.[13]

7 Impact: Report on the police use of facial recognition technology identifies significant concerns – University of Essex, accessed 3rd January 2023: https://www.essex.ac.uk/research/showcase/report-on-the-police-use-of-facial-recognition-technology-identifies-significant-concerns

8 Uncorrected oral evidence: Live facial recognition – Justice and Home Affairs Committee, 12th December 2023: https://committees.parliament.uk/oralevidence/14009/pdf/

9 Independent legal review of the governance of biometric data in England and Wales – Matthew Ryder KC, Ada Lovelace Institute, June 2022: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

10 Uncorrected oral evidence: Live facial recognition – Justice and Home Affairs Committee, 12th December 2023: https://committees.parliament.uk/oralevidence/14009/pdf/

11 Authorised Professional Practice: Live Facial Recognition – College of Policing, 21st March 2022: https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition

12 For example - Clearview AI, a controversial company that has harvested billions of faces from social media platforms and sells these databases to state and private actors around the world: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition

13 Police to be able to run face recognition searches on 50m driving licence holders – Daniel Boffey, the Guardian, 20th December 2023: https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-

7. What methods are used to communicate with the public about police use of LFR? How much information about the use of LFR is shared with members of the public, and is this information easy to find?

Some police forces post on social media as deployments begin. Typically, no advance warning is given to the public, although in some exceptional occasions, such as the King's Coronation, forces will announce the day before that they intend to deploy LFR. SWP no longer posts on social media before or during deployments. Instead, they post deployment updates on their website, meaning they are less accessible to the public.

Signage at deployments, which alerts the public that they are about to walk into LFR's zone of recognition, has also become smaller, and placed in locations making it difficult for the public to have time to avoid cameras should they wish to exercise their right to do so. For example, at the recent deployment of LFR at the North London Derby in September 2023, Big Brother Watch witnessed signage alerting members of the public that they were about to walk into the facial recognition zone that was placed at a point inside the train station which made the technology impossible to avoid when exiting.

8. LFR providers and police forces often mention the need to keep information reserved for safety and commercial reasons. How would you strike a balance between those concerns and the importance of algorithm transparency?

Outsourcing policing to a private-sector algorithm is problematic from a decision-making perspective, and from a transparency perspective. NEC is not subject to the Freedom of Information Act 2000, despite their technology being used to carry out a public function. This has made the independent assessment of the technology's levels of accuracy and bias challenging.

9. How can people who feel that they have been wronged by LFR hold the police to account? How do they find information about how to complain? How frequent are such complaints, and what is the process for considering them?

a. Are the existing complaint systems adequate? (Are there any useful international comparators?)

As noted, the lack of specific legislation overseeing police use of LFR means there is no legal framework and no prescribed route to redress for individuals who have been misidentified by the technology. In our experience attending deployments, people who are misidentified by the technology are held by officers for a significant period of time, have their fingerprints and any ID cards checked and only let go after a significant window of time. However, in order to formally complain or seek legal redress individuals would have to appoint lawyers, engage further with the police and potentially build a legal challenge – something that is inaccessible and impractical for most affected members of the public.

Many people will adversely impacted by LFR, not only by being misidentified and stopped by police officers, but by their being subject to a biometric identity check as they go about their lawful business. At deployments of LFR, Big Brother Watch has spoken to many members of the public who feel deeply uncomfortable about their data being processed in this way. Given the lack of democratic input, members of the public have no way to mitigate this.

12. How widespread is the use of ethics committees?

Checks on police powers should not consist of committees. Lindsey Chiswick, when questioned whether the MPS is obliged to follow the recommendations made by the MPS' ethics committee, admitted that the force was not, but asked "why would we not follow five very good and sensible recommendations"?[14] The other side of this admission is that presumably the MPS would not follow recommendations that they do not consider 'good'. This is illustrative of the weak level of protection ethics committees provide. Given that 40% of ethics committee chairs in England and Wales are also serving police officers, their independence is also questionable.[15] Ethics committees can not, and must not, replace the democratic oversight and legislation that is so urgently needed.

searches-on-50m-driving-licence-holders

14 Uncorrected oral evidence: Live facial recognition – Justice and Home Affairs Committee, 12th December 2023: https://committees.parliament.uk/oralevidence/14009/pdf/

15 Police ethics committees in England and Wales: Exploratory online and web surveys – Paul Snelling et al, *Policing: A Journal of Policy and Practice*, Volume 17, 2023: https://academic.oup.com/policing/article/doi/10.1093/police/paac059/6658660?login=false