Policing Uses of Live Facial Recognition in the United Kingdom

Peter Fussey (University of Essex)
Daragh Murray (University of Essex)

BACKGROUND TO THE USE OF FACIAL RECOGNITION IN THE UK

London has a long history of trialing advanced surveillance technology. Police agencies first installed closed-circuit television (CCTV) cameras in the city in 1953, and until recently London likely had more CCTV cameras per person than any country in the world.[1] The city deployed one of the world's first automatic license plate recognition (ALPR) systems in the mid-1990s, and has since introduced crowd-modeling video analytics to survey its mass transit systems.[2] London was also one of the first cities in the world to trial facial recognition (FR) in the east of the city during the late 1990s, although technological limitations at the time led to its abandonment.[3]

1 Pete Fussey, "Beyond Liberty, Beyond Security: The Politics of Public Surveillance," *British Politics* 3, no. 1 (April 2008): 120–135. See also Jess Young, "A History of CCRV Surveillance in Britain," SWNS, January 22, 2018, https://stories.swns.com/news/history-cctv-surveillance-britain-93449/. London remains the most CCTV-heavy city outside of China.

2 Pete Fussey, "Observing Potentiality in the Global City: Surveillance and Counterterrorism in London," *International Criminal Justice Review* 17, no. 3 (September 1, 2007): 171–192.

3 Pete Fussey, "Eastern Promise? East London Transformations and the State of Surveillance," *Information Polity*, 17, no. 1 (January 2012): 21–34.

With rapid advancements in FR technology, the Metropolitan Police Service (MPS) conducted a series of ten live facial recognition (LFR) test deployments between 2016 and 2019, moving to operational deployments in early 2020.[4] South Wales Police have also been using LFR since 2017, mostly at large concerts, festivals, and sporting events.[5] Both constabularies deploy LFR by installing temporary cameras at a fixed geographic location[6] for a fixed time period.[7] Police generally mount the cameras on an LFR van with a control center used to monitor the live LFR feeds and to communicate with officers on the ground. LFR cameras scan the faces of all individuals passing through their field of vision, and then officers check the resultant biometric profiles against a watch list containing persons of interest. To date, police have only deployed LFR technology in this standalone manner, and have not, for example, integrated it into existing infrastructure, such as CCTV networks.[8]

Police use of LFR has resulted in significant controversy, with a number of human rights and civil society organizations leading opposition against LFR deployments. Many of these organizations have initiated advocacy campaigns calling for either a moratorium on the use of LFR,[9] or an outright prohibition.[10] South Wales Police's use of LFR is currently subject to legal challenge, and an initial hearing before the Court of Appeal took place in June 2020.[11]

In order to examine issues relating to operational effectiveness and human rights compliance, the MPS invited the authors to provide an independent academic report on the last six LFR test deployments.[12] We conducted ethnographic observations from beginning to end of each deployment, of pre-deployment police briefings and post-deployment debriefings, and of a range of other planning meetings. We also held interviews with key stakeholders and analyzed large quantities of MPS internal documents. In this piece, we draw on this research to explore three key themes relating to the regulatory regime: 1) the legal requirement for an authorizing law for LFR; 2) the inability and failure of existing institutions and laws to meaningfully restrict this technology; and 3) the operational considerations unique to LFR. Our focus is on working toward human rights compliance. A key element not addressed in this piece is the "necessity" of police LFR deployments. However, this consideration only comes into play if an appropriate legal basis exists.

---

4 Having moved out of the "test" phase, the MPS now has authority to deploy LFR on the basis of operational intelligence. For further information, see Metropolitan Police, "Live Facial Recognition," n.d., https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

5 For more information, see South Wales Police, "Facial Recognition Helps South Wales Police Become Smarter, Creating a Safer and Connected Community," n.d., http://afr.south-wales.police.uk. The list of deployments is available at https://afr.south-wales.police.uk/wp-content/uploads/2020/04/All-Deployments.pdf.

6 A "fixed location" might be a city square, the entrance to an underground tube station, or a football match, for example.

7 This is typically a number of hours; to date, no deployments have lasted longer than a day.

8 Although this is becoming increasingly technologically feasible, it is unlikely that these more advanced LFR deployments will occur in the short term.

9 See, for example, Carly Kind, "Biometrics and Facial Recognition Technology—Where Next?" Ada Lovelace Institute, July 2, 2019, https://www.adalovelaceinstitute.org/biometrics-and-facial-recognition-technology-where-next/.

10 See, for example, Liberty, Resist Facial Recognition, https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/; and Big Brother Watch, Stop Facial Recognition, https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/.

11 The complaint was brought by Ed Bridges, who believes he was subject to facial recognition processing at a peaceful anti-arms trade protest, and while Christmas shopping. See Liberty, "Liberty Client Takes on Police in Ground-Breaking Facial Recognition Challenge—Hearing Opens Today, May 21, 2019, https://www.libertyhumanrights.org.uk/issue/liberty-client-takes-on-police-in-ground-breaking-facial-recognition-challenge-hearing-opens-today/.

12 Peter Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," University of Essex Human Rights Centre, section 2,1.1, July 9, 2019, http://repository.essex.ac.uk/24946/.

Police LFR deployments directly engage / interfere with several distinct human rights protections. The right to privacy of all individuals passing through a camera's field of vision (and thus subject to biometric processing) is directly engaged. Additional, discrete right-to-privacy issues are raised by any retention or analysis of the resultant footage.[13] The use of LFR may also engage discrimination laws as a result of the technology's biases.[14] Importantly, the deployment of LFR technology may generate a chilling effect, whereby individuals refrain from lawfully exercising their democratic rights due to a fear of the consequences that may follow.[15] This may harm a number of rights, including the right to freedom of expression, the right to freedom of assembly and association, and the right to freedom of religion.[16]

Significantly, the UK's Human Rights Act 1998 (implementing the European Convention on Human Rights[17]), requires that any interference with a right be "in accordance with the law." As such, any measure interfering with human rights protections must have a legal basis, and that legal basis must be of sufficient quality to protect against arbitrary rights interferences. Key in this regard is the foreseeability of the law.[18] If a measure fails to satisfy the "in accordance with the law" requirement, it is unlawful in and of itself.

THE COMMON LAW AS A LEGAL BASIS FOR LIVE FACIAL RECOGNITION

United Kingdom common law establishes the core common law principles for police: protecting life and property, preserving order, preventing the commission of offenses, and bringing offenders to justice.[19] Although no legislation exists that explicitly authorizes police use of LFR, the government has claimed that these common-law powers provide sufficient implicit legal authorization to satisfy the "in accordance with the law" test.

In *Bridges v. South Wales Police*, the UK High Court agreed with the Government,[20] indicating that the common law establishes sufficient legal basis for LFR.[21] This judgment is currently subject to appeal, and this finding is a key point of contention.

---

13 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 59.

14 For further discussion on indirect discrimination, see *D.H. and Others v. the Czech Republic*, Judgment ECtHR, App. No. 57325/00, November 13, 2007, para. 184.

15 The precise contours of any chilling effect are contested, but research points to its existence. See Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31, no. 1 (2016): 117; see also Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* 93, no. 2 (2016): 296–311; for a general discussion, see Daragh Murray and Pete Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data," *Israel Law Review* 52, no. 1 (March 2019): 31–60. For a discussion of the chilling effect as it applies to journalists, see Centro Europa 7 S.R.L. and Di Stefano v. Italy, Judgment, European Court of Human Rights, App. No. 38433/09, June 7, 2012, para. 129.

16 For a more in-depth discussion of potential human rights harms, see Fussey and Murray, "Independent Report," section 2,1.2, http://repository.essex.ac.uk/24946/.

17 See, e.g., *Shimovolos v. Russia*, Judgment, ECtHR, App. No. 30194/09, June 21, 2011, para. 67.

18 *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, January 24, 2019, para. 94.

19 See, for example, Metropolitan Police, "Live Facial Recognition, (LFR) MPS Legal Mandate," p. 5, July 23, 2018, https://www.statewatch.org/media/documents/news/2018/dec/uk-live-facial-recognition-lfr-mps-legal-mandate.pdf.

20 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 78: "For these reasons, we consider the police's common law powers to be 'amply sufficient' in relation to the use of AFR Locate. The police do not need new express statutory powers for this purpose." ("AFR Locate" is South Wales Police's nomenclature for LFR.)

21 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 78.

At the heart of the matter is the fact that police powers under the common law are expressed in broad terms. The common law is inappropriately vague and, for example, does not delimit the circumstances in which a particular measure may be deployed, such that those circumstances are foreseeable, thereby protecting against arbitrary rights interference. Relying on the common law to provide a legal basis for LFR therefore arguably fails to satisfy the "in accordance with the law" requirement established under human rights law, and presents a clear risk of arbitrariness.[22]

A key reason for the High Court's conclusion that the common law was a sufficient legal basis for LFR, and that new statutory powers were not required, was the classification of LFR as a nonintrusive means of obtaining information,[23] and as "no more intrusive than the use of CCTV in the streets."[24] This is clearly contentious: it appears inconsistent with common understandings of the surveillance capacity inherent in LFR, and has been challenged by a number of key figures in the UK. It also appears inconsistent with the High Court's own finding that—as a form of biometric processing—LFR engaged the right to privacy of all individuals passing through an LFR camera's field of vision.[25]

Concerns regarding the arbitrary exercise of powers mean that reliance on the common law to provide the legal basis for the use of LFR is likely to be incompatible with the UK's obligations under the Human Rights Act or European Convention on Human Rights. The Bridges line of cases will provide further guidance in this regard. However, irrespective of the outcomes of these cases, establishing an explicit legal and regulatory basis for the use of LFR would provide much needed clarity, both for the public and for the police.

OTHER LAWS, LEGISLATIONS, AND AGENCIES THAT APPLY TO LFR

Police documentation and political debate have consistently referred to the oversight roles of the multiple data-protection and surveillance-related authorities in the UK.[26] These include the UK's data-protection authority, the Information Commissioner's Office (ICO); the Surveillance Camera Commissioner; the Biometrics Commissioner; and the Investigatory Powers Commissioner's Office. While these agencies have contributed to the debate, each body is narrowly relevant to a specific aspect of LFR and, critically, they do not have explicit authorization to limit LFR deployments. Indeed, while many of these regulatory bodies are heralded as a safeguard to promote appropriate use, their mandates do not provide meaningful oversight. This is explained in the following table:

---

22 This concern is equally applicable vis-à-vis the regulation of LFR deployments. The human rights law tests regarding clarity, foreseeability, and protection against arbitrariness are equally applicable in this regard. This conclusion is supported by relevant case law. See, for example, *S and Marper v. United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, December 4, 2008, para. 99.

23 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 74.

24 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, para. 75.

25 This finding distinguishes LFR as more invasive than CCTV. See *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, September 4, 2019, paras. 59, 62.

26 As noted above, these considerations are irrelevant if the "in accordance with the law" requirement is not satisfied.

Authority	Role	Application to LFR
The Information Commissioner's Office (ICO)	Oversees issues relating to data protection in the UK, particularly the Data Protection Act 2018 and the General Data Protection Regulation.[27] In 2017, they published "In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information," which provided best practices for automated recognition technologies.[28]	Although important, data protection law cannot adequately address the broad range of potential human rights harms brought about by police LFR deployments. It does not, for example, fully address issues relating to whether the use of LFR is necessary or proportionate. As such, the impact of the ICO on the overall LFR debate is relatively limited.
The Surveillance Camera Commissioner	Established by the Protection of Freedoms Act 2012 to oversee the use of closed-circuit television systems (CCTV). [29]	While they are primarily focused on CCTV systems, and LFR is implemented through standalone video systems, they have published guidance on police use of LFR.[30]
The Biometrics Commissioner	Established by the Protection of Freedoms Act 2012 to oversee retention and use of biometric information.[31]	The Biometrics Commissioner's role is restricted in statute to fingerprints and DNA data, and so does not extend to LFR. The Commissioner has published several statements questioning the use of LFR and has said that "we need proper governance of new biometric technologies such as LFR through legislation."[32]
The Investigatory Powers Commissioner's Office	Established under the Investigatory Powers Act 2016, has authority to oversee covert police deployments.[33]	As currently deployed, the principal uses of LFR by police in the UK are not classified as covert. This may change going forward.

27 See, further, the Information Commissioner's Office (ICO), https://ico.org.uk/about-the-ico/.

28 ICO, "In the Picture: A Date Protection Code of Practice for Surveillance Cameras and Personal Information," Version 1.2, June 9, 2017, https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

29 Protection of Freedoms Act ref. See, further, the Surveillance Camera Commissioner, https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about.

30 See, for example, the Surveillance Camera Commissioner's Code of Practice, June 2013, https://www.gov.uk/government/publications/surveillance-camera-code-of-practice; and "The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems," Section 33 Protection of Freedoms Act 2012, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

31 Protection of Freedoms Act ref. See, further, Office of the Biometrics Commissioner, https://www.gov.uk/government/organisations/biometrics-commissioner/about.

32 See, for example, GOV.UK, "Automated Facial Recognition," September 10, 2019, https://www.gov.uk/government/news/automated-facial-recognition, https://www.gov.uk/government/news/biometrics-commissioner-on-the-police-use-of-live-facial-recognition.

33 Investigatory Powers Act 2016, https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

As it stands, police use of LFR in the UK is not subject to adequate oversight or meaningful regulation. This must urgently be addressed.

ISSUES ARISING IN THE CONTEXT OF POLICE LIVE FACIAL RECOGNITION DEPLOYMENTS

This section examines a number of issues arising in the context of LFR deployments, including watch lists, the "presumption to intervene" and associated deficits in effective human oversight, how accuracy is determined, and potential discrimination. These operational elements illustrate the uncertainty associated with LFR deployments, contesting police claims of utility, and highlight problems arising from the absence of appropriate regulation.

Operational Considerations

Measuring LFR performance is complex and includes both partial and instrumental use of statistics. Some technical evaluations compare the number of false matches to an estimate of the total number of individuals passing through an LFR camera's field of vision during a given deployment. These numbers are widely cited by supporters of LFR, yet they offer only a tiny ratio of numbers of faces scanned to those correctly or incorrectly matched.[34] A variation of this approach was adopted by the MPS in a recently published evaluation of their LFR trial deployments,[35] leading to widely publicized claims that the technology was "70% effective."[36] However, such claims often conflate two different forms of data, merging "blue list" data (where volunteers are sent past the cameras to measure their effectiveness—the measure used to support the claim of 70 percent effectiveness) and live data (camera performance when there is no certainty about whether suspects will walk past the cameras).

Another shortcoming of this methodology is the way it de-emphasizes the impact of LFR on those flagged by the technology by contextualizing their experience against larger quantities of data that are arguably less relevant. This makes this measure less suitable for understanding the individual rights-based interferences brought by LFR. Other measures of LFR performance compare how often a human operator discards a computer-suggested alert.[37] One challenge of this approach is the potential for readers to conflate human and computer decision-making: a human might decide the LFR system is wrong, regardless of the veracity of the computational decision.

---

34 See comments by Baroness Williams of Trafford regarding "a one in 4,500 chance of triggering a false alert," House of Lords, January 27, 2020, https://www.theyworkforyou.com/lords/?id=2020-01-27a.1300.2&p=12902.

35 National Physical Laboratory and Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," February 2020, https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf.

36 Vikram Dodd, "Met Police to Begin Using Live Facial Recognition Cameras in London," *Guardian*, January 24, 2020, https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras.

37 Bethan Davies, Martin Innes, and Andrew Dawson, An Evaluation of South Wales Police's Use of Automated Facial Recognition (Cardiff: Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University, 2018).

We designed our independent academic review of the MPS system to address the above challenges, focusing on human rights considerations and protection against arbitrary rights interferences. The research used the same statistics as the MPS study above,[38] and asked two straightforward questions to determine accuracy and examine the role of human oversight:

a. When an LFR system matches someone to the watch list, how often is it verifiably correct?[39]

b. To what extent do human adjudicators consider LFR matches to be credible? To understand if a computer match is correct, it needs to be tested against something—in this case, an identity check of the suspect.

For (a), our research found that out of forty-two computer-generated LFR matches, eight were verifiably correct (19.05 percent). For (b), human adjudicators judged twenty-six out of forty-two matches were sufficiently credible to apprehend the matched individual (61.91 percent), meaning that humans overwhelmingly overestimated the credibility of the system. Four of these matched individuals were lost in the crowd. The remaining fourteen were incorrectly matched by the LFR system.

Two conclusions can be drawn from this. First, there is a "presumption to intervene" on behalf of human operators assessing the credibility of LFR matches. Second, this tendency of deference to the algorithm exists despite the computer being either incorrect or not verifiably correct in a large majority of cases.

These conclusions hold relevance for considerations over the form of human adjudication taking place around LFR systems. Policy emphasizes the importance of "the human in the loop" as a safeguard against algorithmic-induced harms. That human adjudication takes place is not in question, however. The issue at stake is the form it takes, and the degree of critical human scrutiny applied. Moreover, a presumption to intervene suggests LFR frames and structures suspicion ahead of human engagement with the technology.

A final question is whether LFR is discriminatory. UK police forces have made repeated claims that LFR technology is nondiscriminatory in terms of racial characteristics.[40] However, this is a complex issue and covers both the capability of the technology in identifying faces from a range of ethnic groups and the composition of databases of suspects (watch lists). It is difficult for law enforcement agencies to undertake an analysis of sufficient scope to support definitive conclusions. For example, the US National Institute of Standards and Technology (NIST) reviewed 189 facial recognition algorithms and revealed marked "demographic differentials" in the performance of facial recognition algorithms across different ethnicities.[41] Accordingly, claims made in the technical evaluation of the MPS LFR scheme that "differences in FR algorithm performance due to ethnicity are not statistically significant"[42] may arise simply because the total number of matches themselves are not statistically significant.

---

38 Sup. 35.

39 In other words, could it be definitively concluded that the individual identified by LFR matched the individual on the watch list, such as by means of a subsequent identity check?

40 See, for example, public statements by Metropolitan Police Commissioner Dame Cressida Dick, RUSI Annual Security Lecture, London, February 24, 2020. "The tech we are deploying is proven not to have an ethnic bias." Available here: https://rusi.org/event/rusi-annual-security-lecture.

41 Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NIST, December 2019, https://doi.org/10.6028/NIST.IR.8280.

42 National Physical Laboratory and Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," p.4.

According to the MPS statistics, twenty-eight people were engaged by a police officer after being matched by LFR systems across their ten test deployments. We contend that it is impossible to make robust and definitive conclusions over demographic disparities from such small numbers. Concerns over this issue have been most recently articulated in March 2020 in calls by Great Britain's Equality and Human Rights Commission to suspend the use of facial recognition in England and Wales until its impact has been independently scrutinized.[43]

CONCLUSION

This piece highlights three key concerns. First, the legal basis underpinning LFR is inappropriately vague, negatively affecting foreseeability, and arguably failing to meet the "in accordance with the law" test established by human rights law. Second, although a number of UK regulatory bodies engage in this area, there is no dedicated body with authority to limit or effectively oversee LFR deployments. Third, operational realities contest police claims of LFR's utility, the effectiveness of human oversight, and discriminatory outcomes. These highlight the practical consequences and harms arising in the absence of appropriate legal or regulatory frameworks.

43 Equality and Human Rights Commission, "Facial Recognition Technology and Predictive Policing Algorithms Out-pacing the Law," March 12, 2020, https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law.