Cambridge Law Journal, **82(3)**, November 2023, pp. 414–449
doi:10.1017/S0008197323000454

REGULATING USE BY LAW ENFORCEMENT AUTHORITIES OF LIVE FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SPACES: AN INCREMENTAL APPROACH

ASRESS ADIMI GIKAY*

ABSTRACT. *Amid the growing calls for the complete prohibition of the use by law enforcement authorities of live facial recognition (LFR) technology in public spaces, this article advocates for an incremental approach to regulating the use of the technology. By analysing legislative instruments, judicial decisions, deployment practices of UK law enforcement authorities, various procedural and policy documents, as well as available safeguards, the article suggests incremental adjustments to the existing legal framework instead of sweeping regulatory change. The proposed approach calls for adopting national legal rules governing watch lists and introducing spatial, temporal and contextual limitations on the deployment of technology based on the assessment of proportionality and necessity. To enhance the effectiveness of overt surveillance using LFR, the article recommends adopting a transparency procedure that promotes accountability without undermining the objectives of law enforcement. Alternatively, the overt use of the technology should be limited to deterring the commission of crimes and safeguarding public safety, where transparency does not undermine its effectiveness. Limiting the scope of overt use of LFR technology entails that law enforcement agencies primarily utilise covert surveillance, with prior judicial approval, except in urgent cases, as this would improve effective criminal investigation and public safety. The legal adjustments proposed in this article can be implemented through flexible secondary legislation or local policies, rather than rigid statutory rules.*

KEYWORDS: live facial recognition; artificial intelligence; law enforcement; sensitive processing; privacy; overt surveillance; covert surveillance

I. FACIAL RECOGNITION TECHNOLOGY: THE CAPTURE VS REALITY

A closed-circuit television (CCTV) footage shows a male subject attacking a female, preventing her from taking a bus as she tries to resist her aggressor.

*Senior Lecturer in AI, Disruptive Innovation, and Law, Brunel University London. Address for Correspondence: Kingston Lane, Uxbridge, Middlesex, UB8 3PH, UK. Email: asress.gikay@brunel.ac.uk. The author is grateful to the anonymous reviewers and the editor for their invaluable feedback. Any errors are solely the responsibility of the author.

The scene ends with the kidnapping of the female subject, leading the police to issue an arrest warrant for the alleged aggressor. A further investigation reveals that the CCTV footage depicted a partially fabricated event, as the victim had actually boarded the bus and headed home, as confirmed by CCTV footage from the bus.

The story is from the BBC's science-fiction TV series, *The Capture*, which portrays a world of ubiquitous facial recognition CCTV cameras.[1] In *The Capture*, a live CCTV feed is tampered with and smoothly switches from an actual event to a fabricated one in a split second. The intelligence community uses artificial intelligence (AI) software to fabricate evidence (using a method known as "correction").[2] The technology is then used to broadcast to the public a live TV interview with a "deep fake"[3] version of a high government official as though it were an actual interview.[4] *The Capture* dramatises and amplifies the potential dangers of growing surveillance using live facial recognition (LFR) technology.

The first ever case to consider the legality of the use of LFR technology in the UK, *R. (on the application of Bridges) v Chief Constable of South Wales Police*, involved the deployment of LFR by South Wales Police (SWP).[5] In submissions reminiscent of *The Capture*, the appellant's counsel invoked the potential of pervasive CCTV cameras across the nation tracking people's movements to explain the illegality of the SWP's use of LFR.[6] The Court of Appeal declined to engage with the claimant's hypothetical scenario, which it acknowledged "may arise in the future", choosing instead to focus solely on addressing the issue of privacy violation based on the facts presented in the case.[7] However, academics and advocacy groups have shown themselves to be more concerned with dystopian visions, such as those depicted in *The Capture* and this has led them to insist on radical solutions, including a moratorium on the use of LFR or its complete prohibition.[8]

This article argues for incremental regulation of the use of LFR technology in law enforcement, where the current legal framework is progressively adjusted in the light of the potential risks and evidence of

[1] "Introducing The Capture", available at https://www.bbc.co.uk/programmes/p0d02vwc (last accessed 2 January 2023).

[2] M. Hogan, "'Spooks Meets Black Mirror': How The Capture Became the Year's Most Wildly Compelling TV Show", *The Guardian*, available at https:/www.theguardian.com/tv-and-radio/2022/sep/12/how-the-capture-became-the-years-most-wildly-compelling-tv-show (last accessed 2 January 2023).

[3] Bobby Chesney and Danielle Citron conveniently define "deep fake" as "shorthand for the full range of hyper-realistic digital falsification of images, video, and audio": B. Chesney and D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753, 1757.

[4] BBC, "Security Minister Gets Deepfaked on Newsnight | The Capture Series 2 – BBC", available at https://www.youtube.com/watch?v = P4wAO48FzYk (last accessed 2 January 2023).

[5] *R. (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 W.L.R. 5037.

[6] Ibid., at [59].

[7] Ibid., at [60].

[8] M. Ryder, *The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales* (London 2022), 79–80; E. Radiya-Dixit, "A Sociotechnical Audit: Assessing Police Use of Facial Recognition", 66, available at https://api.repository.cam.ac.uk/server/api/core/bitstreams/dea624a6-9337-403d-ae5f-bb151cb07a67/content (last accessed 13 September 2023).

actual harm from using LFR. In the aftermath of the UK Government's publication of a White Paper setting out the country's approach to regulating AI technologies,[9] it is crucial to have clarity on regulating the use of LFR technology in law enforcement. The White Paper adopts a pro-innovation stance towards regulating AI using a sectoral approach. The UK's regulatory trajectory suggests that the Government favours a light touch approach to the existing relevant sectoral laws rather than introducing a sweeping regulatory framework that creates similar regulatory rules and standards for AI systems across all sectors. In line with this, the White Paper envisions regulators implementing five principles in their sectors as they interpret the existing laws: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.[10]

There are conflicting judicial decisions regarding the need to reform the current legal framework governing the deployment of LFR in public spaces. The Divisional Court in *Bridges* held that, despite LFR being a new technology, it does not require the introduction of new laws.[11] The Court of Appeal disagreed with this assessment.[12] Meanwhile, existing studies that propose radical solutions take little interest in looking holistically at the evidence emerging from the actual use of the technology in the UK, and the relevant policies, procedures and safeguards for its deployment. A comprehensive analysis of the available evidence is essential for assessing the suitability of the current legal framework or the extent of legal reform needed to address the challenges that the technology presents.

This article critically analyses the existing literature, laws, codes of practices, policies and procedures followed by UK law enforcement authorities in deploying LFR and Equality Impact Assessment documents, along with the decision in *Bridges*. The article primarily focuses on UK law, occasionally referencing the upcoming European Union (EU) AI Act.[13] The European Parliament's (EP) compromise text outright prohibits using LFR,[14] whereas the European Commission's initial proposal permitted a regulated use of the technology.[15] Despite the Commission's proposal not being adopted by the EP, its rules on facial recognition systems used in law enforcement remain a valuable source of insight.

[9] Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation*, Cm. 815 (London 2023).
[10] Ibid., at 26.
[11] *R. (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), [2020] 1 W.L.R. 672, at [84] (Haddon-Cave L.J. and Swift J.).
[12] *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [90].
[13] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (COM/2021/206 final).
[14] European Parliament, "DRAFT Compromise Amendments on the Draft Report" (2023), 129, available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf (last accessed 13 September 2023).
[15] European Commission, "Proposal for a Regulation", Article 5(2)–(5).

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

The rest of the article is divided into four sections. Section II provides an overview of LFR technology and its risks and benefits. Section III analyses the legal framework that governs the use of LFR technology by law enforcement authorities in the UK and explains the areas that do not require legal reform. Section IV examines areas where legal adjustment is necessary, advocates for incrementalism by setting out its normative framework and offers specific recommendations. Section V concludes the article by highlighting the limit of incrementalism in addressing legal challenges beyond the deployment of LFR technology.

II. LFR Technology in the Context of Law Enforcement

A. The Distinctive Features of LFR

Today, facial recognition technology finds extensive application across both the public and private sectors. Amongst other things, it is used for unlocking mobile phones and tablets, eliminating the need to input passwords manually, authenticating individuals for banking services and conducting automated checks at the border.[16] It is a process by which AI software can identify or recognise a person using their biometric facial features extracted from a photo or video.[17] The software compares the features captured by a camera against an existing biometric facial image to estimate the degree of similarity between two templates.[18] LFR involves six essential steps: compiling/using an existing image, image acquisition, face detection, feature extraction, comparison and matching.[19] Generally, the last five stages, namely image acquisition to matching, should occur instantaneously.[20] The UK police compare the facial features of individuals against images of persons in the police database (a so-called "watchlist").[21]

LFR has at least three distinctive features that present opportunities and risks which must be carefully addressed. First, the instantaneous matching of facial features is one of its unique characteristics. Non-real-time facial recognition, or

[16] Centre for Data Ethics and Innovation, "Snapshot Series: Facial Recognition Technology" (2020), 18, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905267/Facial_Recognition_Technology_Snapshot_UPDATED.pdf (last accessed 13 September 2023).

[17] Information Commissioner's Office, "Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places", available at https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (last accessed 13 September 2023).

[18] Ibid.

[19] *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [9].

[20] However, there could be some delays in the process due to a software flaw or intentional design aimed at circumventing specific rules applicable to LFR. To address this, the EU AI Act recognises that real-time remote biometric identification systems may experience minor delays during analysis, but that such delays do not negate their real-time nature: European Parliament, "DRAFT Compromise Amendments", 140. It should be noted that terms such as "significant delay" and "minor delay" involve subjective assessment that could cause practical challenges.

[21] *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [9].

post-system, involves facial image analysis after the event.[22] In practical terms, this requires an investigating officer to obtain a facial image of the subject from a source such as CCTV and subsequently to compare their facial biometric features with facial biometric data held in a database. The instantaneous identification process may have its downside, as the LFR Operator and LFR Engagement Officer might need to decide to intervene quickly, such as by arresting the subject, creating room for engagement with mistakenly identified persons. However, under the practices of the Metropolitan Police and the SWP established by their Standard Operating Procedures (SOPs), engagement is preceded by human review, where the Engagement Officer, who is notified of an alert by the Operator, has the authority to decide whether to engage with the subject.[23] The EU AI Act mandates that at least two persons must conduct a human review in the case of biometric identification systems, without which an action cannot be taken.[24]

Second, LFR software processes biometric data, which is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data".[25] A video footage or a photo alone does not qualify as biometric data without there being a technical analysis that results in data that uniquely identifies the individual.[26] Such technical analysis aims to extract features including "the width of nose, wideness of the eyes, the depth and angle of the jaw, the height of cheekbones, and the separation between the eyes".[27] As this kind of processing is intrusive, it is considered to be sensitive processing, which thereby requires adherence to strict data protection standards.

Third, LFR technology can process personal data on a mass scale as it is deployed in a publicly accessible space where the faces of thousands of people can be seen and captured. The scale of facial feature analysis by this technology is significant, making it a unique form of surveillance technology.

[22] M. Veale and F. Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" (2021) 22 Computer Law Review International 97, 101.

[23] Metropolitan Police, "Standard Operating Procedure (SOP) for the Overt Deployment of Live Facial Recognition (LFR) Technology", [10.8], available at https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf (last accessed 28 August 2023); see also South Wales Police, "Standard Operating Procedure (SOP) for the Overt Deployment of Live Facial Recognition (LFR) Technology", [10.8], available at https://www.heddlu-de-cymru.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/live-facial-recognition/live-frt-docs-july-23/lfr-sop-v1.2-draft.pdf (last accessed 18 August 2023).

[24] European Commission, "Proposal for a Regulation", Article 14(5).

[25] DPA 2018, s. 205(1).

[26] European Data Protection Board, "Guidelines 3/2019 on Processing of Personal Data Through Video Devices" (2020), [74], available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf (last accessed 14 September 2023).

[27] B.O. Omoyiola, "Overview of Biometric and Facial Recognition Techniques" (2018) 20 IOSR Journal of Computer Engineering 1, 2.

B. Benefits of Law Enforcement Authorities' Use of LFR

Through aiding law enforcement authorities in identifying and locating suspects and vulnerable persons, such as missing children, LFR technology significantly contributes to criminal investigation and public safety.

Facial recognition technology has proven effective in preventing potential threats to public safety, including terrorism. In 2019, an individual left two electric rice cookers in a New York subway station, causing public panic and the evacuation of the transportation hub.[28] A New York Police Department (NYPD) detective used facial recognition technology to identify the suspect using an image from a CCTV camera compared against photos in the police database. By relying on possible matches suggested by the technology and additional manual scrutiny, the NYPD successfully identified and arrested the suspect before it was determined that the rice cookers were harmless.[29] Although this was not a real-time system, it demonstrates that LFR can help avert a threat to public safety through its capability to enhance the swift identification of persons of interest.

During a deployment by the SWP at a public event in 2018, SWP "identified a person who had made a bomb threat at the very same event the previous year and who had been subject to a (suspended) custodial sentence".[30] Besides apprehending criminals, the technology is also used to locate witnesses and the associates of suspects.[31]

Another proven benefit of LFR is the apprehension of individuals with outstanding arrest warrants or those suspected of having committed crime. In nine[32] deployments between February 2020 and July 2022, the London Metropolitan Police Service (MPS) presumably[33] arrested nine subjects.[34] In 2017, the SWP deployed LFR in 13 instances, leading to 15 arrests.[35] In a single SWP deployment in 2022, two cases of arrest/disposal were reported.[36] Without deploying LFR, making these arrests

[28] C. McCarthy, "How NYPD's Facial Recognition Software ID'ed Subway Rice Cooker Kook", *New York Post*, available at https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/ (last accessed 4 January 2023).

[29] Ibid.

[30] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [101] (Haddon-Cave L.J. and Swift J.).

[31] Metropolitan Police, "Standard Operating Procedure", [6.8].

[32] Because one deployment was stopped due to technical fault, no data has been reported in relation to that deployment.

[33] "Presumably" because the Metropolitan Police "LFR Deployments" record states in the relevant table column "arrests/disposals". "Disposal" does not necessarily refer to an arrest: Metropolitan Police, "MPS LFR Deployments 2020 – Date", available at https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf?__cf_chl_tk=E4chFYMwb1R0UEpHQDPXHwY97erNGn7HlaoR4TLWC6E-1672872096-0-gaNycGzNC9E (last accessed 4 January 2023).

[34] Ibid.

[35] South Wales Police, "2017 Deployments", available at https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/FRT-deployments.pdf (last accessed 5 January 2023).

[36] South Wales Police, "2022 Deployments", available at https://www.heddlu-de-cymru.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/all-lfr-deployments-list-march-2022.docx (last accessed 14 September 2023).

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

would otherwise have required considerable police resources. And the swift apprehension of the suspects prevents potential further crimes and safeguards public safety.

Another potential benefit of LFR is the ability to locate vulnerable persons, including missing children and those presenting a risk of harm to themselves or to others.[37] Although there is no data on whether vulnerable persons have been located using LFR in the UK, non-real-time facial recognition has successfully been used to reunite missing children with their parents in India, which demonstrates its potential to help locate vulnerable persons.[38]

An independent study of 11 deployments by the SWP between 2017 and 2018 conducted by Bethan Davies, Martin Innes and Andrew Dawson at Cardiff University concluded that: "The evidence clearly supports the conclusion that AFR [Automated Facial Recognition] processes and systems can contribute to police identifying persons of interest that they would not otherwise have been able to do so."[39] The advantages of LFR outlined above present a compelling case for using this technology for law enforcement purposes. The key focus should be on putting in place a suitable legal framework that enables the safe and responsible use of the technology whilst mitigating its potential risks.

C. Risks of LFR in Law Enforcement

LFR technology carries several risks that could undermine the rights of individuals and the welfare of citizens. Two commonly cited concerns are: the potential for inaccuracy stemming from biased model training datasets;[40] and privacy intrusion and surveillance.[41]

1. Inaccuracy, bias and discriminatory impact

A study by researchers at the US National Institute of Standards and Technology has shown that facial recognition systems are less accurate

[37] Metropolitan Police, "Standard Operating Procedure", [6.8].

[38] A. Cuthbertson, "Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology", *The Independent*, available at https://www.independent.co.uk/tech-india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html (last accessed 5 January 2023).

[39] B. Davies, M. Innes and A. Dawson, "An Evaluation of South Wales Police's Use of Automatic Facial Recognition", 42, available at https://www.statewatch.org/media/documents/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf (last accessed 14 September 2023).

[40] C. Jones, "Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts on People of Color, and the Need for Federal Legislation" (2021) 22 North Carolina Journal of Law & Technology 777, 785–86. See generally G.M. Haddad, "Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom" (2021) 23 Vanderbilt Journal of Entertainment & Technology Law 891.

[41] T. Madiega and H. Mildebrath, *Regulating Facial Recognition in the EU* (Brussels 2021), 32.

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

when identifying certain faces.[42] In a 2018 study, Joy Buolamwini and Timnit Gebru found that commercial gender classification facial analysis algorithms had higher accuracy rates with male faces compared to female faces (8.1 per cent – 20.6 per cent difference in error rate) and performed even better on lighter-skinned faces than darker-skinned faces (11.8 per cent – 19.2 per cent difference in error rate).[43] The algorithms had the poorest performance on darker-skinned female faces (20.8 per cent – 34.7 per cent error rate).[44]

There could be several reasons for the inaccuracy of facial recognition algorithms. The most widely accepted cause of inaccuracy is the limited composition of model training data.[45] If the machine learning system is trained primarily on facial images of lighter-skinned faces, its accuracy decreases when presented with images of people with darker skin. This is commonly attributed to biased data selection, also known as statistical bias,[46] which occurs when data from certain groups are underrepresented in the training dataset.

The implications of inaccuracies in LFR technology could be severe. In the US, law enforcement authorities have used non-real-time facial recognition, leading to numerous mistaken identifications and wrongful arrests of Black Americans. For instance, Nijeer Parks, a Black American, was wrongly identified by a non-real-time facial recognition system, for suspicion of shoplifting, resisting arrest and attempting to hit a police officer with a vehicle, amongst other things, leading to his wrongful incarceration for 11 days in New Jersey.[47] In February 2023, Detroit Police arrested a pregnant black woman, Porcha Woodruff, after she was wrongly identified by the police using facial recognition.[48] The incidents of wrongful arrests based on misidentification by facial recognition in the US are troubling. However, these incidents could be partly attributable to the fact that the regulatory standards of policing in the US are lower compared to the UK and that there is a private prison system in the US, which could potentially lead to higher levels of police misconduct and wrongful arrests.[49]

[42] M. Ngan and P. Grother, "Face Recognition Vendor Test (FRVT): Performance of Automated Gender Classification Algorithms", i, available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8052.pdf (last accessed 14 September 2023).

[43] J. Buolamwini and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1, 8.

[44] Ibid.

[45] Ibid., at 12.

[46] Ryder, *Ryder Review*, [7.29].

[47] J. General and J. Sarlin, "A False Facial Recognition Match Sent This Innocent Black Man to Jail", available at https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html (last accessed 8 January 2023).

[48] A.M. Sahouri, "Lawsuit Filed After Facial Recognition Tech Causes Wrongful Arrest of Pregnant Woman", available at https://eu.usatoday.com/story/news/nation/2023/08/08/facial-recognition-technology-wrongful-arrest-pregnant-woman/70551497007/ (last accessed 14 September 2023).

[49] G.I. Galinato and R. Rohla, "Do Privately-Owned Prisons Increase Incarceration Rates?" (2020) 67 Labour Economics 1.

The National Physical Laboratory independently tested two facial recognition software systems for accuracy, including NEC Neoface V4, which is used by the MPS and the SWP forces, and published the result in 2023. The study is based on data collected through deploying LFR for the purpose of the study, simultaneously(in the same locations) with five deployments by the MPS and the SWP in London and Cardiff respectively.[50] The test confirmed that the LFR systems had the poorest performance on Black-Female faces, but that the discrepancy in accuracy rates across demographics is statistically insignificant.[51] Whilst the result is encouraging, law enforcement authorities should continuously monitor the accuracy of the software they use, alongside putting in place safeguards to address eventual risks of inaccuracy to the public, including minority groups. In this regard, the MPS's existing practice, including the Equality Impact Assessment,[52] shows an encouraging awareness of the potential disproportionate impact that LFR technology could have on specific demographics and efforts to address it. These efforts include: understanding possible discrepancies in the technology's accuracy across demographics; subjecting automated identification to human review; and halting operation in case of suboptimal performance.

Whilst authorities should always prioritise the responsible use of the technology, as of now, no alarming cases of wrongful arrest or abusive engagements with individuals based on misidentifications by a facial recognition system have been reported in the UK.

2. Privacy intrusion and surveillance – room for compromise

The use of LFR in law enforcement could potentially violate the right to privacy. In *Bridges*, the Divisional Court and the Court of Appeal agreed that the SWP's use of LFR interfered with the appellant's right to private life recognised under Article 8 of the European Convention on Human Rights (ECHR) (see Section III(A) below).[53]

In addition, it is feared that the extensive use of LFR by law enforcement authorities could expand a government's surveillance power beyond law enforcement and have a chilling effect on other civil and political rights. Such effects include, amongst others, the stifling of freedom of expression[54]

[50] T. Mansfield, "Facial Recognition Technology in Law Enforcement Equitability Study", 2, available at https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf (last accessed 28 August 2023).

[51] Ibid., at 4.

[52] Metropolitan Police, "Equality Impact Assessment", available at https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-eia.pdf (last accessed 2 April 2023).

[53] *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [131]; *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [62] (Haddon-Cave L.J. and Swift J.).

[54] K.E. Roy, "Defrosting the Chill: How Facial Recognition Technology Threatens Free Speech" (2022) 27 Roger Williams University Law Review 185, 201.

and the suppression of peaceful demonstration and assembly.[55] Along this line, Nathalie Smuha et al. expressed the concern that permitting the use of remote biometric identification systems could lead to the installation of a permanent surveillance infrastructure that could be operational at any moment, leading to privacy interference and a chilling effect on the exercise of democratic rights, including freedom of expression and assembly.[56]

The fear of the potential misuse of LFR technology to suppress democratic rights arises from existing practices in other regions. For instance, in a legal challenge involving an allegation that the use of facial recognition in public spaces led to the arrest of a political protestor, the European Court of Human Rights (ECtHR) found Russia to be in violation of its obligation under the ECHR.[57] In 2022, the Cambodian Government was accused of using drones to intimidate and possibly profile peaceful protestors under the guise of ensuring security.[58] Such practices raise concerns about the potential chilling effect that the deployment of LFR technology for law enforcement purposes might have on democratic rights.

Given the existing precedents elsewhere, it would be imprudent to disregard completely the possibility of mass surveillance using LFR technology meant for law enforcement in the UK. Nevertheless, it is equally crucial to see this in the overall context of the country, particularly the prevailing rule of law that establishes the limits of surveillance. This contextual assessment is essential to understanding the actual capacity of LFR technology to amplify surveillance capabilities.

The paramount aspect to consider is that, within the current legal framework, law enforcement authorities cannot establish an enduring AI-powered surveillance infrastructure in publicly accessible areas that could be activated at will due to the potential for such measures to be deemed disproportionate under the Human Rights Act 1998 (see Section III(A) for further details). Furthermore, the deployment of the technology is subject to limitations regarding time, location and purpose.

Currently, the police deploy LFR by mounting a camera on a marked police vehicle, a pole or other structure, which is then removed after the intended duration.[59] The temporariness and spatial limits of deployment are rooted in Article 8(2) of the ECHR, where the/an infringement of

[55] A. Powers, K. Simon and J. Spivack, "From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong" (2023) 26 Richmond Public Interest Law Review 155, 163.

[56] N. Smuha et al., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", 26, available at https://ssrn.com/abstract=3899991 (last accessed 8 April 2023).

[57] *Glukhin v Russia* (Application no. 11519/20), Judgment of July 4 2023, not yet reported, at [99].

[58] R. Chandran, "Activists Say China's New Silk Road Equips Autocrats with Spy Tech", available at https://www.context.news/surveillance/activists-say-chinas-new-silk-road-equips-autocrats-with-spy-tech (last accessed 30 July 2023).

[59] *R. (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [12].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

privacy should be proportionate to the aim pursued, which limits the power to install live surveillance cameras at whim.

Nevertheless, privacy law alone may not be sufficient to tackle the effect of LFR technology on other civil and political rights. If the threat of the chilling effect of the technology is considered real and imminent, one way to address this would be to create a legal restriction on using the technology in the context of critical civil and political activities, such as demonstrations against the Government or other socio-economically and politically significant events. Such a restriction would tackle censorship and the potential chilling effect of the technology, whilst allowing law enforcement authorities to utilise it in non-political contexts, such as significant sporting events, where credible security threats exist (see Section IV(C)(2) below). These kinds of restrictions should not take the form of a blanket prohibition, as a proportionality assessment needs to be conducted in the given circumstances. Whilst the details must be carefully thought out, the general approach allows for a reasonable compromise.

III. The Existing Legal Framework in the UK

The use of LFR technology by law enforcement authorities in the UK is governed by various legal frameworks. Most of these frameworks are capable of effectively addressing the challenges that the technology presents. This section analyses privacy, data protection, equality and civil liability laws.

A. Privacy Law Under the ECHR

As is well known, following the enactment of the Human Rights Act, public authorities must act in a manner which is compatible with the rights recognised in the ECHR.[60] These rights include the right to respect for private and family life, as well as home and correspondence, enshrined in Article 8 of the Convention.[61] The 1998 Act requires courts or tribunals to take into account the jurisprudence of the ECtHR in determining a question which has arisen in connection with a Convention right.[62]

The ECtHR has interpreted Article 8 broadly in a number of decisions[63] to include a person's physical, psychological and social identities, such as race, gender and sexual identities.[64] Furthermore, the court has made it clear that the right to privacy extends to acts in public spaces,[65] potentially implicating

[60] Human Rights Act 1998, s. 6(1).
[61] ECHR, art. 8(1).
[62] Human Rights Act 1998, s. 2(1).
[63] *Amann v Switzerland* (2000) 30 E.H.R.R. 843, at [65]; *S and Marper v United Kingdom* (2009) 48 E.H.R.R. 50, at [66]; *Pretty v United Kingdom* (2002) 35 E.H.R.R. 1, at [61].
[64] See *S and Marper v United Kingdom* (2009) 48 E.H.R.R. 50, at [66]; *Von Hannover v Germany* (2005) 40 E.H.R.R. 1, at [50].
[65] *Von Hannover v Germany* (2005) 40 E.H.R.R. 1, at [77].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

the use of LFR by law enforcement authorities. In cases, such as *Bridges*, that involve the processing of personal data, the violation of the right to privacy under Article 8 of the Convention can be established if the processing is conducted in such a way that it intrudes into the individual's private life. Previous decisions have found that the recording of personal data in a permanent form[66] or its mere storage can interfere with private life within the meaning of Article 8(1).[67] In this regard, courts consider the individual's reasonable expectation of privacy to be "a significant though not necessarily conclusive factor".[68]

In *Bridges*, SWP argued that there cannot be a reasonable expectation of privacy in a public space, where an image of a person is recorded and processed near-instantaneously, without recording biometric data and making it available to a human.[69] This was rejected by the Divisional Court, which held that the automated capturing of a person's facial image and the extraction of biometric features for comparison with existing biometric data fall under Article 8(1) of the Convention.[70] The Divisional Court apparently recognised a reasonable expectation of privacy in this instance. Although the Court of Appeal did not engage with this question, as it merely summarised the Divisional Court's findings on the issue, it proceeded on the basis that the use of LFR by the SWP interfered with the appellant's right to privacy within the meaning of Article 8(1) of the Convention.

The other controversial issue is whether the interference with privacy falls under the exception in Article 8(2). To fall under this exception, the justification for interfering with private life would need to be (1) in accordance with the law, (2) in pursuit of a legitimate aim and (3) necessary in a democratic society.[71] In *Bridges*, the Divisional Court and the Court Appeal disagreed on this question.

The Divisional Court found that the deployment of LFR met all three requirements of Article 8(2),[72] but the Court of Appeal ruled that the "in accordance with the law" requirement was not met due to a lack of clarity in the legal basis for deploying LFR.[73] The justifications for the police's use of LFR technology are detecting, investigating or prosecuting

[66] *Uzun v Germany* (2011) 53 E.H.R.R. 24, at [47].
[67] *Amann v Switzerland* (2000) 30 E.H.R.R. 843, at [66]–[67].
[68] *Perry v the United Kingdom* (2004) 39 E.H.R.R. 3, at [37].
[69] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [51] (Haddon-Cave L.J. and Swift J.).
[70] Ibid., at [59] (Haddon-Cave L.J. and Swift J.).
[71] ECHR, art. 8(2). See European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence", 10–14, available at https://www.echr.coe.int/documents/d/echr/Guide_Art_8_ENG (last accessed 14 September 2023).
[72] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [101] (Haddon-Cave L.J. and Swift J.).
[73] *R. (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [90]–[91]; B. Keenan, "Automatic Facial Recognition and the Intensification of Police Surveillance" (2021) 84 M.L.R. 886, 890.

crimes and preserving public safety. Because these are considered to be legitimate aims, it is generally not difficult to meet the first condition.[74] The necessity and proportionality of using the technology are assessed on a case-by-case basis, weighing the aim pursued against the effect on privacy.[75] Both courts agreed that the SWP's use of LFR was in pursuit of a legitimate aim and fulfilled the requirements of necessity and proportionality. However, the Court of Appeal held that it failed to meet the "in accordance with the law" requirement for interference with privacy rights (the first prong).[76]

An interference with private life is considered to be in accordance with the law if it fulfils several requirements that the author organises into three general categories. First, the measure must have a basis in domestic law.[77] Second, the law must be compatible with the rule of law requirements of accessibility and foreseeability.[78] Third, the law must afford adequate legal protection against arbitrariness by sufficiently defining the scope and manner of the exercise of discretion by public authorities.[79] The last two requirements are dubbed the "quality of law requirement" in the case law of the ECtHR.[80] A rich body of jurisprudence explains each component of the three general requirements. Of interest to the core argument of this article is identifying why the Court of Appeal concluded that the "in accordance with the law" requirement was not met.

First, the legal basis for privacy-intrusive measures under Article 8(2) need not be statutory law; it can also be a code of conduct or administrative guideline, as long as there are effective means of enforcing them.[81] On this issue, the Divisional Court's conclusion that "[t]he legal framework within which AFR Locate operates comprises three elements or layers (in addition to the common law), namely: (a) primary legislation; (b) secondary legislative instruments in the form of codes of practice issued under primary legislation; and (c) SWP's own local policies",[82] was accepted by the Court of Appeal.[83]

[74] J. Murdoch and R. Roche, "The European Convention on Human Rights and Policing: A Handbook for Police Officers and Other Law Enforcement Officials", 69, available at https://www.echr.coe.int/documents/d/echr/handbook_european_convention_police_eng (last accessed 14 September 2023).

[75] See *Bank Mellat v Her Majesty's Treasury (No. 2)* [2013] UKSC 38, [2014] A.C. 700.

[76] The Court of Appeal was mindful that, because the interference with the claimant's right was not in accordance with the law, no further analysis was necessary, but engaged with the question of proportionality and necessity: *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [131].

[77] *Klaus Müller v Germany* (2021) 73 E.H.R.R. 1, at [48].

[78] *Sunday Times v United Kingdom* (1979–80) 2 E.H.R.R. 245; *Silver v United Kingdom* (1983) 5 E.H.R.R. 347; *Malone v United Kingdom* (1985) 7 E.H.R.R. 14.

[79] See European Court of Human Rights, "Guide on Article 8", 65. *Piechowicz v Poland* (2015) 60 E.H.R.R. 24, at [212].

[80] See generally B. van der Sloot, "The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases" (2020) 11 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 160.

[81] *R. (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9, [2015] A.C. 1065, at [11] (Lord Sumption).

[82] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Ad), at [84] (Haddon-Cave L.J. and Swift J.).

[83] *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [118], [120]–[121].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

The common law confers upon the police the power to collect and retain information for the purpose of maintaining public order and detecting or preventing crimes without a specific search warrant, as long as it does not involve intrusive surveillance.[84] In addition, Part 3 of the Data Protection Act (DPA) 2018, which implemented into UK law the EU Law Enforcement Directive (LED),[85] provides grounds for sensitive personal data processing. The processing of personal data in the case of LFR is considered sensitive as it is aimed at uniquely identifying an individual using biometric data. Although some contentions were made, there was no disagreement that Part 3 of the DPA provides a legal basis for using LFR as long as the relevant conditions were met (see Section III(B) below). Similarly, the Home Office's *Surveillance Camera Code of Practice*,[86] which covers certain aspects of deploying LFR technology, was considered relevant secondary legislation.[87] Last, the SWP's local policies containing the SOP and Sensitive Data Processing Policy were considered to be part of the legal basis for interfering with the appellant's right to privacy, as long as these are published.[88]

Although the aforementioned legal frameworks provide the basis for using LFR, the Court of Appeal ruled that they fail to meet the "quality of law" requirement. Specifically, the local policies of the SWP granted the police unlimited discretion in determining the individuals to be added to the watch list and the deployment locations of LFR.[89] The court emphasised that the "other persons where intelligence is required" category mentioned in the Data Protection Impact Assessment (DPIA) gave the police unlimited discretion in creating the watch list.[90] Regarding the issue of deployment locations, the court pointed out that the lack of a normative requirement or limit on where the LFR technology could be deployed was a flaw.[91] Whilst stressing that the task of designing specific policies is out of its purview, the Court of Appeal concluded that "the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police, and for that reason do not have the necessary quality of law".[92]

The third prong for justifying interference with private life under Article 8(2) is proportionality. Even if the interference is in pursuit of a legitimate aim and in accordance with the law, it may fail the proportionality test. The Court of Appeal, having concluded that the

[84] *R. (Catt) v Association of Chief Police Officers* [2015] UKSC 9, at [7] (Lord Sumption).
[85] Part 3 of the DPA 2018 transposes into domestic law Directive (EU) No 2016/680 (OJ 2016 L 119 p.89).
[86] Home Office, *Surveillance Camera Code of Practice* (first published 2013, London 2021).
[87] *R. (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [109]–[118].
[88] Ibid., at [121].
[89] Ibid., at [123]–[124].
[90] Ibid.
[91] Ibid., at [130].
[92] Ibid., at [94].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

interference with the appellant's private life was not in accordance with the law, engaged with the argument on proportionately (although it did not have to do so) on principle. On this issue, the decision of both courts in *Bridges* largely hinged on whether the use of LFR technology by the SWP met two of the four requirements of the *Bank Mellat* test for proportionality.[93] These requirements are whether a less intrusive measure could have been used without unacceptably compromising the objective of the measure pursued and whether, having regard to the severity of the consequences of the measure, amongst other things, "a fair balance has been struck between the rights of the individual and the interests of the community".[94]

The Divisional Court concluded that the two deployments of LFR by the SWP were proportionate in the light of, amongst other things, the aim pursued, the limited duration and the transparency of the deployments, public engagement, limited personal data processing and the outcomes of the deployments (specifically, the successful arrests of wanted suspects).[95] The Court of Appeal affirmed this conclusion.[96]

In summary, *Bridges* demonstrates that Article 8 of the ECHR adequately addresses the privacy challenges posed by the use of LFR technology by the police. Interfering with private life requires a clear legal basis that meets the standards of the rule of law and limits discretion. This is further analysed in Section IV(C)(1). Courts also need to engage with the proportionality assessment, even if the legal basis for the interference is clear or the objective of the interference is legitimate. There are no inherent characteristics of LFR technology that undermine the effectiveness of Article 8 of the Convention.

B. Data Protection Law

In law enforcement, data processing is governed by the LED which was implemented into UK law by the DPA 2018. The LED's provisions are as good for LFR deployment, as they are for other less advanced personal data processing methods. Currently there is no gap in the provisions of the LED that is uniquely related to the police's use of LFR technology.

Under the LED, processing biometric data – personal data used to identify uniquely a natural person – is considered sensitive processing,[97] requiring adherence to more stringent data processing requirements. Notably, sensitive processing must be: (1) permitted by law;[98] (2) necessary for exercising "a function conferred on a person by an enactment or rule of law"[99] and

[93] *Bank Mellat v HM Treasury (No. 2)* [2013] UKSC 38.
[94] Ibid., at [20] (Lord Neuberger).
[95] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [101] (Haddon-Cave L.J. and Swift J.).
[96] *R. (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [143]–[144].
[97] DPA 2018, s. 35(8), defines sensitive processing.
[98] Ibid., ss. 35(1)–(2).
[99] Ibid., sched. 8, para. 6(2)(a).

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

"necessary for reasons of substantial public interest";[100] and (3) the authority must have an appropriate policy document.[101]

Processing personal data for law enforcement purposes – during the course of an investigation, when prosecuting a crime or when safeguarding public safety – falls within the requirements that processing must be permitted by law and necessary for the reasons of substantial public interest. This means that the first two requirements are usually easily met. To meet the last requirement, the authority should have an appropriate policy document which must be retained, reviewed and updated regularly during the relevant period. This policy document must include, amongst other things, procedures for complying with data protection principles and a policy for the retention and erasure of personal data.[102]

The LED also requires the authority to conduct a DPIA when the type of processing is likely to result in a high risk to individuals' rights and freedoms.[103] The controller must consider the nature, scope, context and purposes of the processing when deciding whether it will likely result in a high risk to individuals' rights and freedoms.[104] The DPIA should include a general description of the processing, an assessment of the risks to data subjects' rights and freedoms, measures to address those risks and safeguards to protect personal data and demonstrate compliance.[105] On this front, the Court of Appeal in *Bridges* (reversing the position taken by the Divisional Court) found the SWP to be in breach of the LED. The reason for this reflected the Court of Appeal's initial conclusion that the use of the technology was not in accordance with the law. In the light of this, it concluded that "notwithstanding the attempt of the DPIA to grapple with the article 8 issues, the DPIA failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found, as required by section 64(3)(b) and (c) of the DPA 2018".[106]

In conclusion, *Bridges* did not expose any gaps in the data protection regime of the LED relating to the police's use of LFR technology. Whilst LFR technology can be used in a way that violates data protection law like any other technology, the use of the technology by law enforcement authorities in itself does not present distinct challenges that the existing data protection law cannot address.

[100] Ibid., sched. 8, para. 6(1)(b).
[101] Ibid., ss. 35(4)(b), 35(5)(c), 42.
[102] Ibid., s. 42.
[103] Ibid., s. 64(1).
[104] Ibid., s. 64(4).
[105] Ibid., s. 64(3).
[106] *R. (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [153].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

C. Equality Law

Although much has been discussed about the disproportionate impact on specific demographics of the use by law enforcement authorities of LFR, there is no strong case for major legal reform to tackle this. The UK has legal rules to tackle discrimination and bias across the public sector.

The ECHR prohibits discrimination on "any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".[107] The Equality Act 2010 requires a public authority, when making decisions of a strategic nature about how to exercise its functions, to have "due regard to the desirability of exercising them in a way that is designed to reduce the inequalities of outcome which result from socio-economic disadvantage".[108] The Act's "public sector equality duty" (PSED) provision requires public authorities to conduct an Equality Impact Assessment to "remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic".[109]

The PSED requires taking positive steps to ensure that decisions and policies made by public authorities do not disproportionately impact specific groups.[110] The Court of Appeal in *Bridges* (again reversing the decision of the Divisional Court) found that the Equality Impact Assessment conducted by the SWP was insufficient as it did not do "everything reasonable which could be done ... to make sure that the software used does not have a racial or gender bias".[111] In spite of the fact that the PSED could be construed strictly to be conditional on the engagement of rights, such as non-discrimination, it is also broader in its scope as it holds public authorities accountable before discriminatory practices that impact individuals occur.

In line with the PSED, the MPS's Equality Impact Assessment provides a comprehensive framework for addressing potential disparities in accuracy based on race, religion, gender, age, sex, disability and other protected characteristics.[112] The document outlines specific measures, including: collaborating with LFR service providers to identify the most suitable software for law enforcement purposes; implementing stringent LFR deployment criteria within the SOP to prevent the targeting of specific individuals or groups; suspending LFR deployment during operations if suboptimal performance is detected; and conducting post-deployment reviews to investigate false alerts and identify patterns or underlying causes.[113]

[107] ECHR, art. 14.
[108] Equality Act 2010, s. 1(1).
[109] Ibid., s. 149(3)(a).
[110] *R.* (*Bridges*) *v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [180] (referring to Arden L.J. in *R. (Elias) v Secretary of State for Defence* [2006] EWCA Civ 1293, [2006] 1 W.L.R. 3213, at [274]).
[111] Ibid., at [201].
[112] Metropolitan Police, "Equality Impact Assessment", 2.
[113] Ibid., at 41.

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

The MPS's Equality Impact Assessment likely satisfies the required standard under the PSED. However, the Equality Impact Assessment should ideally be developed in consultation with a diverse range of stakeholders, including police associations,[114] institutional representatives and members of the broader public through open consultation. Doing so will promote enhanced compliance with the PSED.

Overall, based on the existing legal framework, the Court of Appeal found the SWP's commendable efforts to comply with their PSED to be inadequate. This demonstrates that the current equality law can effectively address the concerns of inaccuracy and bias that are raised by the use of LFR technology by law enforcement authorities, without the need for reform.

D. Civil Liability Laws

Civil remedies for the illegal use of LFR by law enforcement authorities are available under a number of legal regimes. This section considers, in outline, potential civil liability under privacy and data protection laws and the tort of negligence.

In the UK, claimants alleging privacy violations have two possible routes for civil claims. The first is in tort law under the misuse of private information. The second is under the ECHR (claims against public authorities).

In tort law, there is no distinctive "tort of privacy infringement". Because of this, privacy violations have been litigated under breach of confidence[115] and, more recently, under misuse of private information.[116] Generally, to find a breach of privacy in tort, courts ask: (a) whether the claimant has a "reasonable expectation of privacy" concerning the information disclosed; and (b) whether the claimant's interest in maintaining their right to privacy outweighs the defendant's interest in freedom of expression.[117]

As recognised by Nicole Moreham, "whether and, if so, when a person might have a reasonable expectation of privacy in a public place",[118] is a difficult question. A reasonable expectation of privacy, being an objective test, requires taking into account several factors including, but not limited to, "the nature of the information, or activity", "the form in which the information is kept" and "the effect on the claimant" of the disclosure of the information.[119] In *Bridges* and other similar cases, claimants would face two important challenges. First, case law in this area involves the

[114] Various police associations, such as the MPS Black Police Association, the MPS Sikh Police Association, and research institutes such as the Ada Lovelace Institute were consulted in drawing up the MPS's latest LFR equality impact assessment: see ibid., at 19–30.

[115] N.A. Moreham and M. Warby (eds.), *Tugendhat and Christie: The Law of Privacy and the Media*, 3rd ed. (Oxford 2016), [4.01].

[116] Ibid., at [5.01].

[117] See ibid., at [5.14]–[5.20]. See also *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [21]–[24] (Lord Nicholls).

[118] N.A. Moreham, "Privacy in Public Spaces" [2006] C.L.J. 606, 606.

[119] Moreham and Warby (eds.), *Tugendhat and Christie*, [5.22].

misuse of private information through publication or broadcasting[120] or, more broadly, disclosure. In *Bridges*, the information is neither published as in *Campbell*[121] nor broadcast or disclosed to an entity that has no authority to access it. Thus, it is unlikely that an action for the misuse of private information would succeed. There is currently no precedent within UK tort law that offers a civil remedy to claimants whose private information is merely collected, analysed and stored without the disclosure of such information contrary to the claimant's reasonable expectation of privacy. As a result, if the court determines that the information has not been disclosed or published, no cause of action for privacy infringement exists (and there is no need to examine whether the threshold of a "reasonable expectation of privacy" has been reached). This also aligns with the fact that, in such cases, there may ultimately not be a harm for which compensation should be awarded, and indeed that appears to be the case in *Bridges.*

Nonetheless, it is worth examining whether, in all cases of the civil claim in tort law in relation to the use of LFR technology by the police, the lack of disclosure of the information acquired during surveillance should defeat a successful claim for privacy infringement. In other words, if the technology is used in an excessive manner, but the information obtained by the police is not disclosed or published, should a civil remedy in tort be unavailable? This is to be decided by courts in the future. It is possible that the concept of "misuse" of private information might be found to extend beyond situations of disclosure (to include collection and use) for two reasons. First, the origin of misuse of private information has been the doctrine of breach of confidence, from which the former mutated as a separate tort.[122] Breach of confidence clearly precludes the use of confidential information, not just the disclosure of such information.[123] Second, this may have some support in case law. In *Imerman v Tchenguiz*, Lord Neuberger M.R. held:

> It would seem to us to follow that intentionally obtaining such information, secretly and knowing that the claimant reasonably expects it to be private, is itself a breach of confidence. The notion that looking at documents which one knows to be confidential is itself capable of constituting an actionable wrong (albeit perhaps only in equity) is also consistent with the decision of the Strasbourg court that monitoring private telephone calls can infringe the article 8 rights of the caller.[124]

[120] See e.g. *Douglas v Hello! Ltd. (No. 3)* [2005] EWCA Civ 595, [2006] Q.B. 125; *Theakston v Mirror Group Newspapers Ltd.* [2002] EWHC 137 (Q.B.), [2002] E.M.L.R. 22.
[121] *Campbell v MGN* [2004] UKHL 22, at [21]–[24] (Lord Nicholls).
[122] Moreham and Warby (eds.), *Tugendhat and Christie*, [5.09].
[123] T. Aplin et al., *Gurry on Breach of Confidence: The Protection of Confidential Information*, 2nd ed. (Oxford 2012), [15.18]–[15.23].
[124] *Imerman v Tchenguiz* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [68].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

Despite involving the unique circumstances of unauthorised access to files that were subsequently disclosed to a solicitor, *Imerman v Tchenguiz* gives room for extending breach of confidence to cover situations involving the mere acquisition of private information, without further disclosure. Nonetheless, assuming that this is plausible, the claimant still needs to demonstrate that the private information was acquired in violation of a reasonable expectation of privacy or an obligation of confidence. In *Bridges*, the Court of Appeal did not review the question of whether Mr. Bridges had a reasonable expectation of privacy in a public space, as this was not the subject of appeal. The Court of Appeal assumed that the appellant has reasonable expectation of privacy, as concluded by the Divisional Court.[125] However, the threshold adopted in assessing the claimant's reasonable expectation of privacy by the Divisional Court was not particularly high, leaving a room for future decisions to deviate from the decision in *Bridges*, to the detriment of claimants. Thus, it can be concluded that a claim in tort law based on the misuse of private information or its variation would likely face serious obstacles in cases similar to *Bridges*.

Nevertheless, the Human Rights Act provides an avenue to assert a civil claim for breach of privacy.[126] The act allows "a court which has power to award damages, or to order the payment of compensation, in civil proceedings", to grant compensation for the violation of the provision of the ECHR, if the court finds such compensation to provide just satisfaction to the claimant.[127] Therefore, whilst there may be challenges in pursuing a claim of breach of privacy under UK tort law, claimants in cases involving the police's use of LFR technology have an alternative legal avenue under the human rights regime. Because the violation of the right to privacy through an interference with the private life of the claimant under Article 8 of the ECHR does not require disclosure of private information, unlike in tort law, the human rights regime could potentially present less challenges to successfully claiming compensation.

In addition to privacy law, data protection law plays a major role in providing a remedy to an aggrieved person in relation to surveillance technologies. The biggest challenge claimants face in data protection cases is proving harm,[128] especially non-material harm (such as distress). Showing general reluctance to award damages for non-material harms in 2021, the UK Supreme Court decided that a mere loss of control over personal data, without proof of material damage or distress, is not compensable under

[125] *R. (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), at [55].
[126] See e.g. *Andrea Brown v Commissioner of Police for the Metropolis and Chief Constable of Greater Manchester Police* (2016) (involving unlawful surveillance of a police officer).
[127] Human Rights Act 1998, ss. 8(1)–(4).
[128] M.N. Lintvedt, "Putting a Price on Data Protection Infringement" (2022) 12 International Data Privacy Law 1, 13.

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

the General Data Protection Regulation (GDPR).[129] However, despite some inconsistencies in practice among EU national courts concerning the threshold that must be met for a claimant to be entitled to compensation for non-material harm, courts do award compensation for such harm.[130]

In asserting violations of data protection rights arising from the use of LFR technology, individuals may encounter challenges. However, these challenges will not impact individuals affected by the unlawful use of LFR technology in unique ways, as successfully claiming compensation for the breach of data protection law is inherently challenging across the board.

Last, in tort law, the police can be liable for harm suffered due to their wrongful conduct. Whilst the police are not liable for harms inflicted by a third party, on the basis of omission (as a general rule),[131] harms caused due to the police's negligent positive action relating to operational matters are compensable.[132] Thus, the police who wrongfully detain an individual using LFR or conduct a distressing interrogation could be liable in tort law.

Based on the preceding analysis, it can be concluded that there are no gaps in the existing laws that apply to the use of LFR technology by the police that call for a comprehensive legal reform. However, there are missing pieces that should be addressed through an incremental change (see Section IV below).

IV. The Need for Incrementalism

A. Incrementalism: Theoretical Foundation and Insight from Practice

This article acknowledges the need to close some loopholes in the current legal framework in relation to the use of LFR technology by law enforcement authorities, but it argues that changes must be made incrementally. Incrementalism is used as a theoretical framework in financial, environmental and technology regulations.[133] It has also been applied to resolve contemporary legal challenges by using old legal rules. Despite these examples, no literature currently theorises its essential components, scope and limitations.

[129] *Lloyd v Google L.L.C.* [2021] UKSC 50, [2022] A.C. 1217, at [159] (Lord Leggatt). For succinct commentary on the case, see J. Skillen, "Damage in the Supreme Court" [2022] C.L.J. 14.

[130] J. Knetsch, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases" (2022) 13 Journal of European Tort Law 132, 144–45.

[131] See *Hill v Chief Constable of West Yorkshire* [1989] A.C. 53; *Van Colle v Chief Constable of Hertfordshire* [2008] UKHL 50, [2009] 1 A.C. 225. The omission principle does not apply when the police have assumed responsibility: e.g. *Costello v Chief Constable of Northumbria* [1998] 1 All E.R. 550.

[132] *Robinson v Chief Constable of West Yorkshire* [2018] UKSC 4, [2018] A.C. 736; *Rigby v Chief Constable of Northamptonshire* [1985] 1 W.L.R. 1242 (Q.B.); *Knightley v Johns* [1982] 1 W.L.R. 349 (C.A.).

[133] See B.L. Rosenbaum, "The Legislative Role in Procedural Rulemaking Through Incremental Reform" (2019) 97 Nebraska Law Review 762; L.R. Jones and F. Thompson, "Incremental vs. Comprehensive Reform of Economic Regulation: Predictable Outcomes and Unintended Consequences" (1984) 43 The American Journal of Economics and Sociology 1.

Lawrence Cunningham and David Zaring contended that, in the context of the US Government's response to the 2008 Global Financial Crisis, incremental adjustments were a more effective and practical form of regulation than overarching reform.[134] Similarly, in environmental regulation, Robert Glicksman and Sidney Shapiro analysed the practice of incremental regulation in the form of deadline extensions or waivers relating to environmental obligations based on assessing actual harm.[135] They argued that such an approach permits regulators to address specific problems within the context of a particular regulatory domain.[136] Although these works focus on different regulatory fields, they advance the view that, in certain circumstances, regulatory adjustments that gradually tighten or loosen regulatory standards based on actual evidence of harm may be superior to sweeping regulation.

Antonio Franco et al. investigated the effectiveness of extending existing EU legislation to address the challenges presented by nanomaterials.[137] They concluded that incrementalism in such cases can be effective if the necessary legislative amendments are made.[138] In essence, incrementalism in this context involves extending existing legislation to address new technology.

The regulation of automated decisions in consumer credit risk assessment also provides a valuable lesson on how regulators adopt incrementalism. In the EU and the UK, automated decision-making (ADM) in consumer credit risk assessment is regulated by the GDPR,[139] as implemented by the DPA 2018 in the UK. The GDPR's key features in this sphere are the prohibition of certain solely automated decisions and its transparency rules that require the disclosure of information about the ADM in question (the so-called "right to explanation").[140]

The lack of tailored laws governing automated consumer credit risk assessment in the US led to a call for GDPR-inspired laws in the US.[141] Despite such a call, automated consumer credit scoring in the US is governed by existing laws passed decades ago – laws that did not envision

[134] L.A. Cunningham and D. Zaring, "The Three or Four Approaches to Financial Regulation: A Cautionary Analysis Against Exuberance in Crisis Response" (2009) 78 George Washington Law Review 39, 48.
[135] R.L. Glicksman and S.A. Shapiro, "Improving Regulation Through Incremental Adjustment" (2004) 52 University of Kansas Law Review 1179.
[136] Ibid., at 1186.
[137] A. Franco et al., "Limits and Prospects of the 'Incremental Approach' and the European Legislation on the Management of Risks Related to Nanomaterials" (2007) 48 Regulatory Toxicology and Pharmacology 171.
[138] Ibid., at 182.
[139] Regulation (EU) No 2016/679 (OJ 2016 L 119 p.1). Articles 2(1), 14, 15, 22 and Recital 71 of the GDPR are the most important provisions governing automated decision-making.
[140] See generally G. Malgieri, "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations" (2019) 35 Computer Law & Security Review 1.
[141] V.E. Hertza, "Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?" (2018) 93 New York University Law Review 1707, 1730.

advanced machine learning algorithms.[142] These laws include the Equal Credit Opportunity Act (ECOA),[143] the Fair Credit Reporting Act (FCRA)[144] and the Fair Housing Act.[145] One of the concerns raised regarding these laws has been that algorithms will allow financial institutions to use information, such as Zip codes, as "a proxy for race" and engage in discriminatory practices that these laws are not designed to address.[146] In response, the Federal Trade Commission issued a guideline specifying that using Zip codes in consumer credit scoring could be challenged under the ECOA.[147]

Although the ECOA does not explicitly address discriminatory practices using Zip codes,[148] the Act has been applied to cases of discrimination that excluded minority neighbourhoods under the practice of redlining,[149] where financial institutions divided these communities according to their Zip codes in loan provisions. In one case, the Justice Department and Consumer Financial Protection Bureau (CFPB) made Hudson City Savings Bank pay over $27 Million in settlement for excluding majority Black and Hispanic counties through redlining.[150]

Similarly, the FCRA has been used to address automated consumer credit reporting issues. In 2017, the CFPB fined Conduent Business Services, L.L.C. $1.1 Million for inaccurate consumer credit reporting using an automated process.[151] Conduent furnished automated consumer credit reporting to lenders and credit reporting agencies in relation to auto loans.[152] The information it provided was used to determine whether consumers qualified for loans or under what terms, but there were errors in the files of over one million consumers, including wrong reports of involuntary repossession of vehicles or account default-related information.[153] The CFPB applied old laws to address this challenge.

[142] A.A. Gikay, "The American Way – Until Machine Learning Beats the Law?" (2021) 12 Case Western Reserve Journal of Law, Technology & the Internet ii, 48–50.
[143] 15 U.S.C. 1691.
[144] 15 U.S.C. 1681.
[145] 42 U.S.C. 3604.
[146] Hertza, "Fighting Unfair Classifications", 1726.
[147] A. Smith, "Using Artificial Intelligence and Algorithms", available at https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms (last accessed 1 July 2023).
[148] ECOA, s. 701.
[149] See generally A. Gano, "Disparate Impact and Mortgage Lending: A Beginner's Guide" (2017) 88 University of Colorado Law Review 1109.
[150] US Department of Justice Press Release, "Justice Department and Consumer Financial Protection Bureau Reach Settlement with Hudson City Savings Bank to Resolve Allegations of Mortgage Lending Discrimination", available at https://www.justice.gov/opa/pr/justice-department-and-consumer-financial-protection-bureau-reach-settlement-hudson-city (last accessed 2 July 2023).
[151] Consumer Financial Protection Bureau, "CFPB Fines Xerox Business Services $1.1 Million for Incorrect Consumer Information Sent to Credit Reporting Agencies", available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-fines-xerox-business-services-11-million-incorrect-consumer-information-sent-credit-reporting-agencies/ (last accessed 6 July 2023).
[152] *In re* Conduent Business Services, L.L.C., CFPB No. 2017-CFPB-0020, available at https://files.consumerfinance.gov/f/documents/cfpb_conduent-business-services_consent-order_112017.pdf (last accessed 14 September 2023).
[153] Ibid., at [10]–[11], [27]–[28].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

Consumer credit scoring practices continue to evolve, due to the extensive datafication of the market and the reliance on machine learning algorithms that collect and analyse consumers' personal data to make predictions in opaque manners.[154] The use of advanced data analytics techniques and opaque machine learning systems in consumer credit risk assessment remains a challenge even in the UK and the EU where the legal frameworks governing personal data and consumer credit are relatively robust.[155] Nevertheless, there does not seem to be a call for major legislative change, as proposals focus on better enforcement, including the issuance of compliance and enforcement guidance by relevant authorities.[156]

The preceding analysis shows that, whenever potential solutions are available within the existing laws to address new technologies, it has become common practice to apply the existing laws rather than to rush to implement new ones. If interpretation by the judiciary or administrative agencies is insufficient, the relevant regulator issues guidelines extending the existing law to the new phenomenon. A new statutory law should only be enacted where such an incremental process does not offer a legal framework that meaningfully tackles the risks posed by the new technology, provided that those risk are also realistically proven to materialise. The author's theory of incrementalism calls for an iterative, continuous and gradual adjustment of the law to address the challenges posed by LFR technology in law enforcement.

B. A Normative Framework for Incrementalism

Whilst incrementalism is addressed in the existing literature and observed in practice, there is no clear guidance on how the theory should be applied in practice. The UK Government's envisioned approach to AI regulation outlined in the White Paper, despite its flaws, incorporates the key components of incrementalism.

Building upon the existing literature, insights from the application of incrementalism in regulating ADM in consumer credit services in the US and the key components of the UK's envisioned AI regulation, the author proposes that incrementalism should incorporate four main ingredients: sectoralism; reliance on existing legal frameworks; evidence-based regulation; and flexibility.

1. Sectoralism

Incrementalism favours a sectoral approach to regulation rather than an overarching regulatory framework that applies to the use of facial

[154] N. Aggarwal, "The Norms of Algorithmic Credit Scoring" [2021] C.L.J. 42, 58–62.
[155] Ibid.
[156] Ibid., 65–73.

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

recognition or AI technologies across the board. Substantive rules should be tailored to a specific sector, whilst the relevant sectoral regulator should be charged with enforcement.

The UK's envisioned AI regulatory approach advocates applying five principles for each regulator to implement in its sectors. Each regulator should determine which principle it should implement or to what extent, depending on what is lacking in the existing legal framework. The fact that these principles may not be backed by the statutory duty to enforce them is, at least initially,[157] problematic.[158] Nevertheless, one of the policies behind the UK's envisioned approach is sectoralism, which creates substantive rules that are adaptable to each sector and enforced by the relevant regulator. Such an approach has several benefits, the main one being its efficient and effective implementation and enforcement.

Entrusting regulatory oversight to a single regulator operating across multiple sectors could result in an inefficient implementation and enforcement system. Regulatory agencies possessing expertise in specific fields are better placed to regulate the AI systems used in their sectors.[159] Centralising regulation may lead to corruption, regulatory capture or misaligned enforcement objectives, impacting multiple sectors. By contrast, a decentralised approach allows specific regulators to set enforcement policies, goals and strategies, preventing major enforcement failures and promoting accountability. In addition to allowing effective oversight, sectoral regulation could help minimise disruption and cross-sectoral regulatory conflict. It can also be formulated at a more granular level, offering better opportunities for effective implementation.

An incremental regulation of the use of LFR technology by law enforcement authorities requires a sectoral-level legal adjustment rather than bringing it under a broad and multi-sectoral single regulation.

2. Reliance on existing legal frameworks

Incrementalism also requires finding solutions in the existing legal framework that should be interpreted to apply to new challenges. The UK's envisioned approach to AI regulation allows regulators to apply the existing regulatory frameworks in conjunction with the principles set out in the White Paper.[160]

This article has argued that there are currently no significant legal loopholes in the existing legal frameworks governing the use of LFR technology by the police that warrant substantial legal reform. If supplemented by appropriate

[157] Department for Science, Innovation and Technology, *Pro-Innovation Approach*, [11].
[158] A.A. Gikay, "How the UK Is Getting AI Regulation Right", available at https://theconversation.com/how-the-uk-is-getting-ai-regulation-right-206701 (last accessed 23 July 2023).
[159] Letter from D. Castro and J. New to E. Connelly (15 February 2019), available at https://www2.datainnovation.org/2019-ftc-competition-consumer-protection.pdf (last accessed 2 July 2023).
[160] Department for Science, Innovation and Technology, *Pro-Innovation Approach*, 17.

guidance and policies, these frameworks can be interpreted to address the challenges posed by LFR technology in law enforcement.

3. Evidence-based regulation

Another essential component of incrementalism is its openness to evidence-based regulation. Legal adjustments should be made based on evidence of actual harm rather than conjecture.[161] LFR technology used by law enforcement in the UK has potential risks. However, the actual risk of harm in some regards, such as the discriminatory impact on specific demographics, is yet to be demonstrated by evidence from actual practice.

For example, the risks of inaccuracy and bias identified in gender classification AI systems[162] are frequently cited to support a moratorium on using LFR in the UK until a comprehensive statute is enacted.[163] Such a call is not based on solid evidence of harm. In its "Stop Facial Recognition" campaign, Big Brother Watch asserts that "Met and South Wales Police facial recognition [are] over 85% inaccurate 2016-2023".[164] Big Brother Watch looked at multiple deployments and the number of false alerts generated relative to the total number of matches.[165] An independent review of the MPS's six deployments between 2016 and 2019 by Peter Fussey and Daragh Murray, which shows a success rate of only 19.05 per cent,[166] is also widely used to highlight the potential risk posed by LFR technology. The reported figures of inaccuracy of LFR technology used by the UK police are alarming in the light of the fact that, due to misidentification by face recognition systems, several incidents of wrongful arrests and incarcerations have been documented in the US. However, it is crucial to put the reported inaccuracy of the technology in the context of the existing safeguards and actual police practice, as well as the overall benefit of the technology.

Fussey's and Murray's report shows that, out of 42 matches generated, 16 were immediately ruled as false alerts without engaging with the subjects, 22 were stopped for an identity check, 14 were ruled as false positives after an engagement and eight were true positives. This means that 63.64 per cent of the individuals stopped for identity checks (14 out of 22) were stopped incorrectly and 36.36 per cent (eight out of 22)

[161] Glicksman and Shapiro, "Improving Regulation", 1179.
[162] See generally Buolamwini and Gebru, "Gender Shades".
[163] Ryder, *Ryder Review*, 80.
[164] Big Brother Watch, "Stop Facial Recognition", available at https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ (last accessed 22 July 2023).
[165] Big Brother Watch Team, "Understanding Live Facial Recognition Statistics", available at https://bigbrotherwatch.org.uk/2023/05/understanding-live-facial-recognition-statistics/ (last accessed 29 August 2023).
[166] P. Fussey and D. Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", 10, available at https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf (last accessed 22 July 2023).

stopped for identity checks matched the individuals wanted by law enforcement.[167] Most of the reports on the inaccuracy of LFR technology focus on false alerts in general, even if the false alerts that are generated are inconsequential in real terms due to the police generally not engaging with most of the subjects falsely identified. If false alerts were to be considered as indicative of potential harm, then the primary focus should be on the number of false alerts where the police engaged with subjects mistakenly identified. At least in such cases, the inaccuracy of the technology arguably starts to manifest an actual effect on individuals. Nonetheless, it is equally crucial to look at how the engagement takes place (e.g. respectful engagement with subjects compared to ill-treatment). With all factors considered and at this stage of the technology, the aforementioned audit did not reveal information that might be damaging to the use of LFR by the police. Identifying eight wanted criminals out of the 22 that had their identities checked is a good result in terms of enhancing public safety.

Regarding differences across demographics, the study by the National Physical Laboratory concluded that LFR systems had the poorest performance on images of Black-Female faces but the discrepancy in accuracy rates "by gender, by ethnicity, and by gender-ethnicity combined were not statistically significant".[168]

Without evidence of actual harm resulting from the use of LFR technology, the anticipated risk of harm based solely on its high inaccuracy rate is insufficient to justify the prohibition of the technology or a major legal reform. This is more so given the series of legal and procedural constraints adopted by UK police, such as Equality Impact Assessment and SOP, which mitigate the potential consequences of mistaken identification. Incrementalism allows regulators to evaluate progressively the risk of harm and make regulatory decisions that are sensitive to the evidence and context.

4. Flexibility

Finally, incrementalism advocates adopting a more flexible regulatory option rather than a route that requires a lengthy legislative process. The UK Government's envisioned approach to AI regulation supports this as well. It favours a non-statutory regulatory framework where regulators initially implement the identified principles without a statutory duty. If the principles set out in the White Paper were to be established through primary legislation, adapting them and swiftly responding to new risks would be challenging due to lengthy parliamentary procedures. The UK Government's envisioned approach is certainly not ideal if the

[167] Ibid., at 70.
[168] Mansfield, "Facial Recognition Technology", 4.

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

notion of a non-statutory enforcement policy, where regulators are not under a statutory duty to enforce the selected principles, is adopted for a prolonged time. Nevertheless, a middle ground exists between allowing regulators to pick principles they choose to enforce on a voluntary basis and rigid, overarching statutory rules.

In summary, incrementalism would be instrumental in ensuring that regulation weighs the risks and benefits of LFR technology and strikes a fair balance based on evidence. It also keeps the door open for changes that respond to the needs of the time. Furthermore, in the context of technology that has demonstrated significant benefits, incrementalism allows for creating a regulatory framework that encourages socio-economically useful innovation. Finally, this approach aligns with the UK Government's current proposed approach to AI regulation, which aims to incentivise innovation.[169]

Based on the preceding, four specific issues need to be addressed: (1) a national rule for watch list; (2) spatial and contextual limits on deployment; (3) adopting appropriate transparency or limiting the scope of overt surveillance; and (4) authorisation of covert deployment by an independent authority.

C. Incrementalism Applied to the Use of LFR by Law Enforcement Authorities

1. National rules for watch list

Generally, due to the potential risks associated with using LFR in public spaces, its deployment should be limited to specific types of crimes and the protection of vulnerable individuals (as legally defined).

The initial European Commission proposal for the EU AI Act allows for LFR to be deployed for: (1) targeted searches "for specific potential victims of crime, including missing children"; (2) "the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack"; and (3) "the detection, localisation, identification, or prosecution of a perpetrator or suspect" of a crime with a maximum sentence of at least three years that would allow for issuing a European Arrest Warrant.[170] The first two requirements in the EU AI Act are similar to the ones that UK police generally adopt. However, the last requirement is more specific and stringent. Currently, the persons on the watch list created by the MPS or the SWP are broader, with no requirement that the use of LFR be confined to offences of a particular gravity.

[169] Department for Science, Innovation and Technology, *Pro-Innovation Approach*, [3].
[170] European Commission, "Proposal for a Regulation", Article 5(1)(d).

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

The MPS and SWP have revised their SOPs following the decision in *Bridges*. Their revised SOPs, which are based on the LFR Authorised Professional Practice (APP) developed by the College of Policing,[171] have similar criteria for including persons in the watch list. Accordingly, a watch list could comprise individuals that meet the criteria set by the relevant parts of the SOPs.[172] These include those who are:

a) wanted by the courts;
b) suspected of having committed a crime or suspected, based on reasonable grounds, to be about to commit a crime or in the course of committing a crime;
c) "subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the deployment";
d) missing and deemed to be at increased risk;
e) at risk of causing harm to themselves or others; and
f) victims of an offence, reasonably suspected to have information of importance and relevance to progress an investigation, or otherwise close associates of an individual and that individual themselves would fall within paragraphs (a) – (f).[173]

The category of persons included in a watch list is generally limited to the closed list provided in the SOP. Therefore, the current rules for the creation of a watch list remove discretion from law enforcement authorities in relation to the persons that can be included in the watch list. However, there is a lack of specification of the types of crimes that warrant the deployment of LFR. In this regard, the police are expected to conduct the assessment of necessity and proportionality by considering other less intrusive methods, the importance of locating the person being sought and expectation of privacy.[174] However, this does not necessarily remove discretion in relation to extending the use of LFR technology for relatively minor crimes.

[171] College of Policing, "Live Facial Recognition: Authorised Professional Practice", available at https://www.college.police.uk/app/live-facial-recognition (last accessed 16 September 2023).

[172] Metropolitan Police, "Standard Operating Procedure", [6.8]; South Wales Police, "Standard Operating Procedure", [6.8]. A single watch list could include individuals who belong to one or more, or even all, of the categories outlined in points (a) to (f), as each point pertains to different categories of individuals.

[173] Ibid. It is worth noting that, in relation to close associates, the MPS's SOP cross-references paragraphs (a)–(e) while the SWP's SOP cross-references paragraphs (a)–(f). Consequently, under the SWP's SOP, close associates include individuals related to the victim of an offence (para. (f)), whereas the MPS's SOP appears to exclude persons related to the victim of an offence from the definition of close associates. In theory, the MPS's SOP seems arbitrary, considering that there is no practical difference between missing persons (para. (c)) or those at risk of harm (para. (d)), on the one hand, and victims of offences (para. (f)), on the other. However, in practice, both police forces' SOPs are likely to be interpreted to yield similar results.

[174] Metropolitan Police, "Standard Operating Procedure", [6.16]; South Wales Police, "Standard Operating Procedure", [6.20].

Excluding certain offences from warranting the deployment of LFR technology is necessary to maintain proportionality between the use of technology and the crime being investigated. The technology should be reserved for severe and high-priority crimes with clear implications for the safety or economic well-being of the public. Giving police unlimited discretion in creating a watch list could lead to inefficient resource allocation, potentially shifting the focus from prioritising the quality of policing efforts to quantifying success based on the number of resolved crimes, no matter how petty the offences might be. This could divert attention from serious crimes, such as murder, rape, human trafficking, tax evasion, money laundering and other financial crimes often involving sophisticated schemes and tech-savvy criminals.

To ensure the effective and responsible use of LFR technology, there needs to be a legal rule that establishes a clear requirement of non-deployment for certain offences. This could be achieved through a national policy document or APP similar to the one developed by the College of Policing that outlines key principles and policies that govern the watch list to ensure consistency in application. The rule should also contain an exception that allows the police to operate flexibly.

2. Spatial, temporal and contextual limits on deployment

It is crucial to deploy LFR in a publicly accessible space where it does not have a disproportionate chilling effect, ideally limiting it to locations where members of the public have low expectation of privacy. Furthermore, the deployment space must be justified based on the reasonable likelihood of the people on the watch list being in the area. Deployments should also have specific temporal limitations. Such limitations align with the proportionality requirement under Article 8(2) of the ECHR.

The SWP has introduced a revised and principled approach to determining the place of deployment[175] in response to the Court of Appeal's decision that the local policy failed adequately to address the place of deployment. In an encouraging step, besides recognising the need for a temporal limit, the SWP's "Legal Mandate" document identifies places where members of the public generally have a higher expectation of privacy and clarifies that deployment in such places requires a proportionality assessment.[176]

While it is not advisable to impose a broad restriction on the deployment of LFR technology in specific places, as it could have a disproportionate

[175] South Wales Police, "South Wales Police Live Facial Recognition (LFR): Legal Mandate" (2023), [4.8], available at https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/live-facial-recognition/live-frt-docs-july-23/lfr-legal-mandate-v1.2-draft.pdf (last accessed 15 January 2023).

[176] Ibid., at [4.11].

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

impact on public safety, it is prudent to consider limitations on LFR deployment in particularly sensitive locations, such as religious institutions, schools and similar venues. These limitations should be determined through a thorough assessment of necessity and proportionality. Adopting such a context-based limitation does not require the enactment of primary legislation, although a national approach would be necessary to ensure the consistent protection of civil liberties across the country.

3. Appropriate transparency, overt use of LFR and the alternative

Under the Home Office's *Surveillance Camera Code of Practice*, people in public spaces normally have the right to be informed if they are being monitored by a surveillance camera system (so-called "overt surveillance"). This includes knowing the authority undertaking the surveillance and the purpose for which the information is to be used.[177] Whilst the *Surveillance Camera Code* requires transparency in overt surveillance,[178] it does not dictate the specific means by which the transparency is to be ensured.

In practice, law enforcement authorities inform the public of LFR use through appropriate channels, including through signs placed before individuals enter the LFR camera's zone of recognition.[179] Additionally, following the LFR APP, the MPS and SWP commit to notifying the public of the deployment of LFR in advance of the operation including through websites and social media.[180] However, a notification through websites and social media is not carried out if it "would undermine the objectives or operational imperative of the deployment".[181] Law enforcement authorities use these transparency obligations to allow members of the public to exercise their right to avoid overt surveillance by not entering the zone of recognition.[182]

Nonetheless, the existing legislation does not state that the goal of transparency in overt surveillance is to enable members of the public to avoid surveillance operations. The overall objective of transparency that can be gathered from the reading of the *Surveillance Camera Code* seems to be that of enabling members of the public to hold authorities accountable, for instance in case of possible abuse.[183] To that end, knowing the authority that conducts the surveillance, the private information acquired, the purpose of the surveillance and appropriate channels for complaints are crucial.

[177] Home Office, *Surveillance Camera Code*, 11. See also Home Office, *Covert Surveillance and Property Interference: Revised Code of Practice* (London 2018), [3.36].
[178] Home Office, *Surveillance Camera Code*, 11.
[179] Metropolitan Police, "Standard Operating Procedure", [5.8]; South Wales Police, "Standard Operating Procedure", [5.8].
[180] Metropolitan Police, "Standard Operating Procedure", [5.9]; South Wales Police, "Standard Operating Procedure", [5.7].
[181] Ibid.
[182] Metropolitan Police, "Standard Operating Procedure", [5.10]; South Wales Police, "Standard Operating Procedure", [5.9].
[183] Home Office, *Surveillance Camera Code*, 11–12.

In practical terms, this means that the police should be open about using LFR technology in public spaces, so as to give members of the public the opportunity to exercise their right to hold the police accountable in relation to possible illegal surveillance. This does not necessarily require the police to enable members of the public, potentially including those suspected of committing crimes, to avoid the surveillance and thereby undermine the very objectives of conducting the surveillance.

Whilst the current level of transparency in overt use of LFR lacks legal basis in primary legislation and could undermine the effective apprehension of wanted criminals, overt surveillance could still prevent criminal activities, as the presence of LFR cameras could act as an effective deterrent in most instances.[184] However, the principal aim of the police's use of LFR technology seems to be to apprehend criminal suspects.[185] With growing public awareness and the police notifying the public of LFR operations before they enter the recognition zone, the overt deployment of LFR may not be achieving its intended objectives, as the procedures followed could potentially provide career criminals with an advantage to strategically avoid these operations.

Evidence from the deployment of LFR in the UK seems to be consistent with the proposition that overt deployment is becoming less effective. In the most recent eight deployments by the MPS (from April to June 2023), with over 97,000 faces estimated to have be seen, only five true alerts were generated, leading to two arrests.[186] This is lower than the 26 true alerts generated in eight deployments in 2022 (see Section II(B) above). However, on a closer look, the evidence is rather inconclusive as the difference in true alert rates could be due to factors, such as crowd size, the size of the watch list, the time of deployment and other environmental factors. Reliable empirical evidence will only be generated by studies covering a more prolonged period, accounting for varying factors impacting the effectiveness of deployments. Nonetheless, the existing literature recognises that transparency in law enforcement, including surveillance, may reduce the effectiveness of law enforcement efforts.[187] If law enforcement authorities aim to use LFR effectively in a covert manner, it is therefore imperative that they revise their SOPs that currently impose excessive transparency requirements.

If law enforcement authorities are not willing to adopt a realistic transparency procedure due to concerns of potential legal challenge,[188]

[184] M. Priks, "The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway" (2015) 125 The Economic Journal F289, F289, F303.

[185] This is the case, even though the watch lists usually contain persons at risk (vulnerable persons).

[186] Metropolitan Police, "MPS LFR Deployments 2023 - Date", available at https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-grid-2023-v.3.1-web.pdf?trk=public_post_comment-text (last accessed 25 October 2023).

[187] B. Buechel, Eberhard Feess and Gerd Muehlheusser, "Optimal Law Enforcement with Sophisticated and Naive Offenders", 3, available at https://www.unifr.ch/amabe/fr/assets/public/Buechel_Feess_Muehlheusser_Deterrence_Feb2019.pdf (last accessed 22 July 2023).

[188] In *Bridges*, the claimant alleged that the deployment of LFR was brought to their attention when they were in close proximity to an LFR-equipped police van, though it was too late to avoid it, but this was not

then they should resort primarily to covert use of LFR technology. Surveillance is covert if "it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place".[189] Under the Regulation of Investigatory Power Act 2000 (RIPA), directed surveillance is one of the recognised forms of covert surveillance.[190] It is undertaken:

(a) for the purposes of a specific investigation or a specific operation;
(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation.[191]

Covert surveillance is subjected to higher oversight as it poses a greater risk to privacy, requiring two-tiered authorisation. Accordingly, to be lawful, directed surveillance must be authorised by designated persons,[192] meaning "individuals holding such offices, ranks, or positions with relevant public authorities"[193] or police of a certain rank in law enforcement.[194] However, such authorisation is ineffective until the relevant judicial authority approves it.[195] In the case of covert intrusive surveillance,[196] authorisation becomes effective once approved by a Judicial Commissioner.[197]

Law enforcement authorities' use of LFR technology could be classified as directed surveillance (if done covertly), as it is used for specific investigations or operations that lead to the acquisition of private information. Because "private information" is defined broadly as information relating to private or family life,[198] LFR systems deployed in public spaces would likely lead to obtaining such information, as affirmed in *Bridges*, where the deployment was considered to have violated Article 8(1) of the ECHR. Moreover, a typical LFR deployment is not made as an immediate response to an event, making it a clear case of directed surveillance.

considered to be one of the important factors in the case: *R.* (*Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058, at [27].

189 RIPA, s. 26(9)(a).
190 Ibid., ss. 26(1)(a), 26(2).
191 Ibid., s. 26(2).
192 Ibid., s. 28(1).
193 Ibid., s. 30(1).
194 Ibid., s. 30(4) and sched. 1(A); Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521, sched. 1.
195 RIPA, s. 32A(2).
196 Intrusive surveillance refers to covert surveillance that "(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device": ibid., s. 26(3).
197 Ibid., s. 36(2)(a).
198 RIPA, s. 26(10).

https://doi.org/10.1017/S0008197323000454 Published online by Cambridge University Press

The alternative solution being proposed here requires limiting the overt use of LFR technology in public places to two specific purposes (as a general rule): locating vulnerable persons; and preventing crimes in general or violence by monitoring public events to prevent threats to public safety. This limited overt use of LFR would be effective because vulnerable persons and persons going to public events with violent intent are unlikely to avoid LFR deployment areas. As such, the transparency of these types of operations does not compromise their effectiveness. For such deployments, the current system of authorisation of overt deployment by law enforcement authorities should be retained, namely authorisation should be given in these cases by the law enforcement authority with no need for additional approval.

In conclusion, the overt use of LFR to apprehend people suspected of committing crimes could prove to be ineffective unless law enforcement authorities adopt a more pragmatic approach to their transparency commitment. The current practice of transparency appears to undermine the objectives of law enforcement authorities' use of the technology. Because of this, law enforcement authorities should mainly utilise covert deployments following the two-tier authorisation procedure applicable to directed surveillance under RIPA, with the exceptions analysed above.

4. Prior judicial approval under RIPA

One of the critical aspects of conducting surveillance is prior authorisation. In the UK, a distinction is made between overt and covert surveillance, in regard to authorisation.

As mentioned earlier, directed (covert) surveillance requires authorisation by the law enforcement authority and judicial approval.[199] For overt surveillance, the *Surveillance Camera Code of Practice*, issued under the Protection of Freedoms Act 2012,[200] allows the Chief Police Officer to establish a procedure of authorisation for the deployment of LFR,[201] with no need for further judicial approval. In normal circumstances, authorisation is granted by a police officer ranked Superintendent or higher. In cases of urgency, an officer below the rank of Superintendent but not below the rank of Inspector could grant the authorisation.[202] That authorising officer must, as soon as practicable, inform a Superintendent or higher of the deployment of LFR who can decide to cease the operation.[203]

On the one hand, the UK's approach to authorising the overt deployment of LFR poses a risk of abuse of police authority since there is no

[199] Ibid., s. 32A(2).
[200] Protection of Freedoms Act 2012, s. 29.
[201] See also Home Office, *Surveillance Camera Code*, 18.
[202] Metropolitan Police, "Standard Operating Procedure", [4.4]–[4.8]; South Wales Police, "Standard Operating Procedure", [4.1]–[4.8].
[203] Ibid.

independent scrutiny. On the other hand, requiring prior authorisation from an independent judicial body could significantly delay deployment, potentially jeopardising public safety. However, the approval of the use of LFR technology as an investigative tool by an independent oversight body could enhance public trust in law enforcement.

In line with the recommendation for the police to rely more on covert surveillance, it would be good practice to employ covert deployment of LFR authorised by the police and approved by the court through an expedited procedure. The procedure should also allow a post-use judicial approval of covert deployments, in cases of justified urgency.[204] To be clear, this proposal does not suggest that the police abandon overt surveillance even for apprehending violent criminals, as noted earlier. It invites law enforcement authorities to be mindful of the fact that the current level of transparency to which they adhere could unnecessarily undermine the effectiveness of law enforcement operations and that they use covert operations as a matter of good practice. This will also better enhance the effective investigation of crimes and public safety.

V. The Limit of the Incremental Approach

The UK law regulating the use of LFR technology by law enforcement agencies has some gaps that require incremental reform. Local policies or codes of practice should be implemented to address these loopholes. To ensure the consistent protection of civil liberty, a national policy that regulates the creation of watch lists should be adopted, in addition to principled limits on the spatial and contextual deployment of LFR involving the assessment of proportionality and necessity. LFR technology should also be reserved for serious offences, excluding minor crimes and SOPs should clearly set out this principle. Judicial approval of authorisation of deployment should be mandatory for covert use, with the possibility for fast-track or post-deployment approval in cases of urgency. To enhance the effectiveness of overt use of LFR, law enforcement authorities should adopt a transparency procedure that is aimed at promoting accountability rather than undermining the effectiveness of law enforcement objectives. Thus, the current level of transparency should be revisited. Alternatively, law enforcement authorities should primarily use covert deployment of LFR, with overt use being limited to specific cases, such as locating non-offending subjects or preserving public safety.

Whilst an incremental approach is a valuable tool in addressing the legal lacunae relating to the deployment of LFR, it has limit in regulating the technology more widely. In the future, it would be necessary to

[204] This procedure is available for intrusive surveillance: see RIPA, s. 35(3)(b) (in case of urgency, the authorisation of intrusive surveillance is effective without a Judicial Commissioner's approval).

implement a regulatory framework requiring companies to develop the technology for law enforcement agencies or, in general, to comply with standards regarding bias in machine learning, transparency, explainability, audibility and accountability, among others. Where there is no existing legal framework that can address these concerns – and currently, there is none – incrementalism may not help to address the regulatory gap adequately as the theory works on the assumption that there is some basis for legal adjustment in the existing legal framework. Where the regulatory gap is significant, a major legislative overhaul would be more fitting.