The Need for Regulation: Permissive Governance and Disproportionate Use of Live Facial Recognition Technology by the Metropolitan Police Service

Thesis submitted for Master of Philosophy in Law

John Thomas Croker

29,911 words

January 2024

Abstract

The use of facial recognition technology by police presents a range of risks to the enjoyment of human rights across society. Human rights law assists legislators to understand the legal parameters for how this technology can be used without undermining the rule of law and its use leading to widespread state surveillance.

The focus of this thesis, the use of live facial recognition (LFR) by the Metropolitan Police Service (MPS) in London, is an example of the risks posed by police use of AI. MPS invokes the language of human rights in justifying their use of LFR, without ensuring appropriate safeguards are in place to protect rights and prevent widespread surveillance. The MPS has used LFR since 2016, and this use threatens the enjoyment of a range of protected rights, including Article 8 of the European Convention on Human Rights (the protection of private and family life).[1] While the technology itself poses novel challenges to the enjoyment of a range of rights, the contribution made by this thesis highlights the risk of police ineffectually self-regulating their use of artificial intelligence (AI) tools without ensuring effective oversight, accountability or appropriate rights protections. The conclusions reached in this thesis call for appropriate and effective regulation and oversight of police use of LFR to ensure rights are protected from unlawful and disproportionate harm.

[1] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), Art 8(1).

Declaration

I certify that this is my own work, and it has not previously been submitted for any assessed qualification.

John Croker

January 2024

Acknowledgements

Studying at Oxford has been a dream of mine since I was a child, when I visited with my family. Of the many people I wish to thank for supporting me in my studies, first and foremost it is them. Thanks to my Dad, Michael and Stepmum, Sarah, who were both able to enjoy the wonders of Oxford with me during my time living and learning here. Thanks to my siblings Eleanor, Elizabeth, Callum and Edith, and my beautiful niece Frankie and nephew Sacha.

Thanks to my Mum, Peggy, who sparked in me a joy of learning and of the law. And particular thanks to my Yiayia, Terpsi Nickoludis who has always given me love and support during my studies and in life.

Thanks to the many people at Oxford who supported me in my research, including my supervisor Professor Martin Scheinin, researchers at the Bonavero Institute including Shreya Atrey, and my examiners Professor Kate O'Regan and Dr Nora Ni Loideain. My thanks also to the support from my work, particularly from Sascha Gelfand, and to Detective Chief Inspector Jamie Townsend for the many stimulating discussions about this important intersection of technology, policing and human rights.

Thanks to my academic mentors Judge Hilary Charlesworth and Professor Simon Rice. Thanks also to Rotary International, and particularly David Gorman, for supporting my studies with a very generous scholarship to take up my research.

Oxford is an amazing place, but the life of a research student can be an isolating one. I am particularly thankful for the love and support I have received from my dearest friends Katie Pentney and Carlos Zelada Acuna, as we shared this experience together with laughter and friendship.

And finally my thanks and love to Stefanie and Sago for their love and support during my studies.

Contents

Abstract.....**ii**
Declaration.....**iii**
Acknowledgements.....**iv**
List of Abbreviations.....**vii**
Table of Cases.....**viii**
UK Cases.....viii
European Court of Human Rights Cases.....viii
Table of Treaties, Conventions and Legislation.....**x**
International Treaties.....x
UK Statutes.....x
Table of Diagrams.....**xi**
Introduction | The Need for Regulation: Permissive Governance and Disproportionate Use of Live Facial Recognition Technology by Police.....**1**
Central Thesis Contention.....4
Structure of Thesis.....4
Methodology.....10
Contribution to Existing Literature.....11
Chapter 1 | LFR Use by the MPS.....**14**
FRT Forms and Uses.....14
Operational Deployment and Authorisation of LFR.....15
Chapter 2 | Article 8 ECHR Jurisprudence: Privacy, Surveillance and Police.....**22**
Article 8 ECtHR Jurisprudence: Overview.....24
Summary of Article 8: Sequential Elements to Assess Lawfulness of LFR.....25
Article 8: Scope of the Right.....26
Gaughran and *Glukhin*.....28
Gaughran v UK.....29
Glukhin v Russia.....33
Applying Article 8 Jurisprudence to the Use of LFR by the MPS.....38
Chapter 3 | Application of Article 8 Safeguards to the MPS's Use of LFR.....**41**
Interference with Article 8(1).....42
Article 8(2): Lawful interference.....46
Police and Criminal Evidence Act.....48
Bridges v South Wales Police: Lawful Authority for LFR?.....52
Legal Authority: 'Consent'.....55
Legitimate Aim.....59
Rational Connection to Legitimate Aim.....64
Evaluation of Accuracy and Bias.....65
Necessity, Proportionality and Fair Balance.....73
Conclusion.....**95**
Bibliography.....**98**

List of Abbreviations

AI	Artificial intelligence
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FRT	Facial recognition technology
GDPR	General Data Protection Regulation
LFR	Live facial recognition
MPS	Metropolitan Police Service
NPL	National Physical Laboratory
OFR	Operator instigated facial recognition
PSED	Public Sector Equality Duty
PSNI	Police Service of Northern Ireland
RFR	Retrospective facial recognition
UN	United Nations

Table of Cases

UK Cases

R (Catt) v Commissioner of Police of the Metropolis [2015] UKSC 9

R (on application of Edward Bridges) v Chief Commissioner of South Wales Police [2019] EWHC 2341

R (on the application of Edward Bridges) v Chief Commissioner of South Wales Police [2020] EWCA civ 1058

R (Gillan) v Commissioner of Police for the Metropolis [2006] UKHL 12 (8 March 2006)

R (Wood) v Commissioner of Police for the Metropolis [2009] EWCA Civ 414

European Court of Human Rights Cases

Barthold v Germany, App no 8734/79 (ECHR 25 March 1985)

Big Brother Watch and Ors v UK App nos 58170/13, 62322/14, and 24960/15 (Grand Chamber, 25 May 2021)

Gaughran v UK App no 45245/15 (EHCR, 13 February 2020)

Glukhin v Russia App no 11519/20 (ECHR, 4 July 2023)

Herczegfalvy v Austria App no 10533/83 (ECHR 24 September 1992)

Klass and others v Germany App no 24952/94 (ECHR, 6 September 1978)

López Ribalda and others v Spain App nos 1874/13 and 8567/13 (ECHR Grand Chamber, 17 October 2019)

Merabishvili v Georgia App no 72508/13 (ECHR Grand Chamber 28 November 2017)

Pavlov and others v Russia App no 31612/09 (ECHR, 11 October 2022)

PG and JH v UK App no 44787/98 (ECHR, 25 September 2001)

PN v Germany App no 74440/17 (ECHR, 11 June 2020)

S & Marper v UK App nos 30562/04 and 30566/04 (Grand Chamber, 4 December 2008)

Sunday Times v UK App no 6538/74 (ECHR 26 April 1979)

Szabó and Vissy v Hungary App no 37138/14 (ECHR, 12 January 2016)

Tyrer v United Kingdom App no 5856/72 (ECHR, 25 April 1978)

Roman Zakharov v Russia App no 47143/06 (Grand Chamber, 4 December 2015)

Table of Treaties, Conventions and Legislation

International Treaties

Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950 (European Convention on Human Rights)

International Covenant Civil and Political Rights, 16 December 1966

Universal Declaration of Human Rights, 10 December 1948

UK Statutes

Equality Act 2010

Human Rights Act 1998

Police and Criminal Evidence Act 1984

Table of Diagrams

Diagram 1: Concept of zone of recognition from MPS governance.....17

Diagram 2: The LFR process utilised by the MPS.....18

Diagram 3: Legal authority diagram: MPS governance.....48

Diagram 4: Public notices of LFR use by MPS in London, July 2022.....56

Diagram 5: LFR deployment Notting Hill Carnival 2017.....91

Introduction | The Need for Regulation: Permissive Governance and Disproportionate Use of Live Facial Recognition Technology by Police

Police use of artificial intelligence (AI) poses a range of risks to human rights. This thesis seeks to critically interrogate one form of AI use that police currently use: live facial recognition (LFR), and the range of risks that it poses to human rights. Specifically, the thesis contends that the self-regulation of LFR use by the Metropolitan Police Service (MPS) in London results in ineffective rights protections and unlawful limitations of a range of protected rights, particularly Article 8 of the European Convention on Human Rights ('Article 8'), the protection of private and family life. The jurisprudence of the European Court of Human Rights (ECtHR) sets out the safeguards and standards to assess the lawful interference with Article 8. Applying this jurisprudence to the governance published by the MPS in support of their use of LFR illuminates the gaps between these legal norms and the adverse rights impacts that result from the police use of the technology. The analysis outlined in this thesis can guide regulators (particularly the Parliament) in legislating for appropriate controls and oversight of the use of LFR by police. A legislated framework to govern LFR use by police will result in a better balance between harnessing the benefits of the technology while also ensuring such use does not undermine the enjoyment of rights and the protection of the rule of law.

Police are often required to locate and apprehend individuals in the community to achieve their law enforcement objectives. This could include, for instance, apprehending a person in connection to a serious crime under investigation, for an outstanding warrant, or for not complying with bail/remand conditions. Facial recognition technology (FRT: the umbrella term for all forms of facial recognition, including LFR) presents a form of surveillance technology that can assist police in these and other circumstances. FRT is also a form of surveillance that can severely undermine human rights if not used lawfully, in a manner that clearly achieves a legitimate objective, and proportionately. This tension, between policing objectives and individual rights, is a common foundation to scholarship and

human rights advocacy that seeks to understand the role of police in democratic societies, and is especially acute here in light of the scale and computational power that drives FRT.

Delineating between lawful and unlawful uses of LFR is consequently a matter of degree, and requires important judgments to be made as to what this technology should lawfully be used to do, and what is clearly disproportionate and unjustified in a democratic society governed by the rule of law. Importantly, the potential for chilling effects and adverse impacts across the community where these technologies are used without effective regulation and oversight is such that regulation must not be left to the police alone. It is proper for the Parliament, as the elected arm of government, to determine the appropriate balance between law enforcement expediency and rights protections. The courts, including the ECtHR, can and should ensure that any such regulatory framework complies with legal requirements. One framework that can assist policy makers to understand how to regulate police use of this technology is human rights law, with its established safeguards and jurisprudence relating to the interference with relevant rights, including the right to privacy.

This thesis draws upon the European Convention on Human Rights (ECHR), and specifically Article 8, in critically engaging with the use of LFR by police. Article 8(1) provides that '[e]veryone has the right to respect for [their] private and family life, [their] home and [their] correspondence'.[2] The right is not unlimited. Article 8(2) sets out the permissible restrictions of the general right by providing that:

> [t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[3]

[2] European Convention on Human Rights, Art 8(1).

[3] European Convention on Human Rights, Art 8(2).

Jurisprudence from the ECtHR has established the relevant legal tests that apply where the legislative or administrative actions of Contracting States interfere with Article 8. This legal analysis requires a two-part assessment. First, the applicant must establish that the impugned action interferes with their right to private and family life. Where the interference is made out, it is for the public authority to establish that the interference is lawful, necessary to achieve a legitimate aim, and proportionate in light of its rights impacts.

This thesis utilises the established Article 8 jurisprudence to argue that the governance model utilised by the MPS in its use of LFR is deficient, resulting in unlawful interferences with the protection of private and family life. The MPS has utilised FRT (including LFR)[4] since 2016 and has published all relevant governance documents justifying its usage of this technology.[5] LFR presents significant risks that can lead to surveillance at scale and resultant human rights breaches if it is not appropriately regulated.

Utilising Article 8 jurisprudence allows legislators to understand the contours of what effective regulation of LFR use by police should entail. It also highlights for advocates the avenues that exist to challenge the use of LFR by the MPS.

Central Thesis Contention

The central contention of this thesis it that the current use of LFR by MPS is disproportionate and unlawful, in light of its interference with human rights. The MPS has itself devised the regulatory framework to govern its own use of LFR. This framework is broad and permissive, and authorises a wide range of deployment and use cases. The MPS purports to use LFR lawfully by relying on existing common law and statutory powers relating to community safety, addressing and investigating crime, and using and processing custody

[4] FRT is the overarching acronym referring to the cluster of technologies that use facial biometrics for identification purposes. LFR is one form of FRT, other forms include 'operator initiated' facial recognition, and retrospective facial recognition.

[5] Metropolitan Police Service, 'Advice and Information: Facial Recognition' (*Metropolitan Police Service*) <https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition> accessed 1 August 2022. Many other policing services, particularly outside the UK, have disclosed little about their use and justification for using this technology. The MPS is accordingly a useful case study for the human rights analysis undertaken in this thesis, with the resultant analysis able to be extrapolated to other policing contexts.

photographs.[6] Rather than clearly delineating between the lawful and unlawful uses of this technology, the MPS framework invokes the language of human rights law but fails to ensure that meaningful human rights protections result from its use.

Structure of Thesis

Chapter 1 introduces the case study this thesis is based on: the use of LFR by MPS. LFR is used in public places overtly by the MPS across London using dedicated vans equipped with high-definition CCTV cameras. The MPS governance of LFR is outlined to understand police use of the technology.

The MPS governance model for LFR permits the exercise of broad discretions by police in the planning and deployment stages, allowing the inclusion of almost any person of interest to police to be included on the watchlist of wanted persons that the technology relies upon. The MPS governance allows police to include any person 'at risk to themselves or others' on the watchlist, alongside other broadly formulated categories for inclusion, such as individuals who may have committed offences (including summary offences), those who may have witnessed crimes, and even individuals who may have been the victim of crime.[7] Similarly, the location of LFR deployments is broadly formulated, presenting no 'red-line' deployments beyond which the surveillance could not be used.[8]

Chapter 2 provides the legal framework of the thesis, using Article 8 jurisprudence from the ECtHR. The purpose of this chapter is to set out the relevant legal principles relating to police use of LFR. This will provide the legal foundation for the critical analysis in

[6] Metropolitan Police Service, 'Live Facial Recognition: Legal Mandate' (Version 2.0) <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-legal-mandate.pdf> accessed 15 June 2022.

[7] Metropolitan Police Service, 'MPS LFR Policy Document: Direction for the MPS Deployment of overt Live Facial Recognition Technology to locate person(s) on a Watchlist' (Version 2.0), <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document.pdf> accessed 15 June 2022, 27 – 28.

[8] See, for example, the broad categories provided in relation to the geographical approval of LFR deployments: Metropolitan Police Service, 'Standard Operating Procedures for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology' (Version 2.0), <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf> (accessed 15 June 2022), [7].

Chapter 3. The elements of Article 8, and its application to different forms of state surveillance, are explored through a series of key cases. Two recent decisions from the ECtHR that apply the Court's Article 8 jurisprudence to facial biometric storage and use by police are summarised in depth: *Gaughran v UK*[9] ('*Gaughran'*) and *Glukhin v Russia*[10] ('*Glukhin'*). In *Gaughran*, the ECtHR was asked to assess the lawfulness of the retention of biometric data (including facial biometrics recorded via custody photographs) of an individual who was convicted of a drink driving offence. It is of particular relevance as the ECtHR recognised the utility of photographs capturing facial biometrics for authorities in light of facial recognition technologies and the corollary impact that such retention and processing will have on the enjoyment of Article 8 rights. In *Glukhin*, the ECtHR determined that the apparent use by police of FRT[11] in identifying and locating an individual who had staged a protest on the Moscow Metro amounted to an unlawful interference with a number of rights including Article 8.

Chapter 3 applies a doctrinal legal analysis of the Article 8 jurisprudence to the case study. The chapter commences by considering whether there is an interference with Article 8(1). The thesis contends that the creation of the watchlist using sensitive biometric data of wanted people interferes with the Article 8(1) right, as does the processing of sensitive biometric data (during the deployment) of all people who pass through the 'zone of recognition' (i.e., the field of vision of cameras that are of a sufficiently high definition to process the live images of the faces of people who pass the cameras). Further interferences arise when alerts are issued by the LFR algorithm, resulting in the exercise of police powers to detain the individual identified by the technology. This may, in turn, lead to further rights intrusions for the affected persons as police exercise powers to ascertain the person's identity before determining whether they should be arrested or not.[12]

9 *Gaughran v UK* App no 45245/15 (EHCR, 13 February 2020).

10 *Glukhin v Russia* App no 11519/20 (ECHR, 4 July 2023).

11 Both LFR and retrospective facial recognition technologies.

12 This may include the use of portable fingerprint scanners that MPS use to check identity: Mayor of London – London Assembly, *Questions to the Mayor: 'Use of Fingerprint Scanners in the Met* (16 July 2020), <

This analysis then turns to whether the MPS has addressed the legal thresholds within Article 8(2) such that their use of LFR amounts to a lawful interference with the right. It is argued that the governance and deployment model used by the MPS does not comply with these legal standards. This includes MPS processes established for the watchlist creation; for the approval of deployments of the technology throughout London; for the role of police in responding to, and apprehending, individuals who are identified by the algorithm; and issues stemming from the outputs of the algorithm (which are discriminatory against individuals of certain genders and ethnicities). Each aspect of LFR deployment gives the police too much discretion at the expense of effective rights protections being mandated by the MPS governance. Similarly, each aspect inadequately addresses the legal burden on police at each stage to identify and balance rights impacts against their operational objectives they seek to achieve in using the technology.

Chapter 3 also interrogates and contextualises the decisions from the United Kingdom (UK) High Court and Court of Appeal in *Bridges v South Wales Police* (‘*Bridges’*), in which the use of LFR by police was found to be unlawful in two key respects (the breadth of discretion wielded by police in relation to who could be added to the watchlist, and where LFR could be deployed).[13] Rather than this outcome leading to the MPS discontinuing their use of the technology, the *Bridges* decisions are used by the MPS in its claim that a legal basis exists to support its use of LFR, stemming from the scope of the powers afforded to the office of constable established in cases such as *R (Catt) v Commissioner of Police of the Metropolis* (‘*Catt*’).[14]

This chapter also includes a discussion of the legal basis claimed by the MPS to use LFR, which rests on the common law and pre-existing statutory powers that allow police to obtain, store, and use still photographs of people in police custody. These laws and powers

https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/use-fingerprint-scanners-met-1> accessed 1 June 2023.

[13] *R (on the application of Edward Bridges) v Chief Commissioner of South Wales Police* [2020] EWCA civ 1058, [209].

[14] *R (Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9, [26].

are ill-suited to addressing the risks posed to Article 8 by LFR, and do not result in strong legal protections or appropriate oversight of the use of the technology by the MPS.

Establishing the legality of Article 8 interferences that result from the MPS's use of LFR requires more than proving the existence of a domestic legal basis for its use. The MPS must also demonstrate the interference is compatible with the rule of law and that the governance in place to regulate its use protects individuals from arbitrary interferences with their rights, including the protection of private and family life. In addition, the MPS must ensure the law relied upon is sufficiently clear and available such that it is foreseeable to individuals who are affected by its use.[15] This thesis engages with each aspect in turn and concludes that the MPS model insufficiently addresses each requirement.

Article 8 also requires public authorities to demonstrate that any interferences further a legitimate aim. This presents some legal risk for the MPS model. A preliminary analysis would suggest that the MPS would be able to satisfy this requirement in any legal challenge. This is particularly the case in light of the specified aims established in Article 8(2) that align with the purported use cases for LFR outlined in the MPS governance, including where the technology is deployed in the interests of public safety, national security, for the prevention of disorder or crime and for the protection of the rights and freedoms of others.[16] However, the accuracy and operation of LFR presents some challenges for the MPS in meeting this requirement. Biases and inaccurate outputs of AI usually engage human rights analysis relating to the right to equality and non-discrimination.[17] The discriminatory outputs of this technology, particularly demonstrated through the reduced efficacy the tool has in accurately identifying people of colour and women, can also result in unlawfulness where the MPS is unable to demonstrate the surveillance furthers a legitimate aim (namely, the *accurate* identification of wanted persons).

---

[15] *R (Gillan) v. Commissioner of Police for the Metropoli*s [2006] UKHL 12 (8 March 2006) [52].

[16] European Convention on Human Rights, Art 8(2).

[17] The right not to be discriminated against in the enjoyment of the rights set forth in ECHR is enshrined in Article 14 ECHR, while Article 1 of Protocol No. 12 to the ECHR prohibits discrimination more generally, in the enjoyment of any right set forth by law. The UK is not a party to Protocol 12.

Some of the specified use cases established by the MPS governance do demonstrate a clear connection between the use of LFR surveillance and achieving a legitimate aim. It is not clear that this threshold is met, however, for other use cases, such as the use of LFR to identify wanted persons in relation to offences where police have *no* intelligence to suggest the person may be located proximate to the deployed cameras, or where the tool is used to track a person whose gender and ethnicity is not accurately identified by the tool (such as a woman of colour).[18]

The final stage of analysis asks whether the interference is necessary in a democratic society. This includes a proportionality assessment balancing the public policy objectives sought to be achieved using the technology against the impacts on the human rights of affected individuals. It also entails consideration of whether a less restrictive option is available to the MPS to achieve the specified legitimate aims without impacting on the Article 8 rights of affected individuals as significantly as LFR does.

The use of LFR technology, particularly in processing large volumes of sensitive biometric data of people passing the deployed cameras and in processing the biometrics of individuals who are on the watchlist, is also arguably disproportionate and unlawful. The MPS governance does not require an assessment of the proportionality impacts on the human rights of affected individuals who are not on the watchlist, but only on those whose biometrics are processed at either the planning, authorisation or deployment stages.[19] This is a significant omission that results in ineffectual rights protections resulting from MPS use of LFR.

This thesis contends that potential unlawfulness of MPS use of LFR can be identified at each stage of an analysis applying Article 8 jurisprudence. While the jurisprudence

[18] National Physical Laboratory, 'Facial Recognition Technology in Law Enforcement Equitability Study: Final Report', Dr Tony Mansfield, March 2023, NPL Report MS 43, 5.

[19] For example, the 'Authorised Officer' is directed to assess 'offence types' rather than the 2000 or more individual people proposed to be included on a watchlist before deployments. This means MPS does not consider the impact on Article 8 and other human rights of individuals before decisions are made, but instead assesses broadly similar considerations on the public interest reasons to include individuals on the watchlist: MPS LFR Policy Document, (n 7), 27 – 28.

relating to LFR use by police under the ECHR continues to develop, the current state of the law illuminates the disproportionate impacts on rights that result from the MPS governance model. This analysis provides guidance for what effective regulatory governance and oversight must entail if governments seek to ensure that the use of LFR does not undermine human rights and the rule of law. The overarching contention of this thesis is that the purported governance framework designed by the MPS to 'regulate' its use of this technology is ineffective in protecting rights. Adequate and appropriate rights protection requires regulation and oversight established by statute that enshrines the thresholds and governance required to ensure LFR use complies with Article 8 standards set in the ECtHR jurisprudence.[20]

Methodology

This thesis seeks to synthesise and apply Article 8 jurisprudence from the ECtHR to the use of LFR by MPS. It is doctrinal as it seeks to apply relevant caselaw and legal standards to the case study.

A doctrinal approach utilising Article 8 jurisprudence is warranted in critically engaging with this case study, as the legal framework relied upon by the MPS is not based on statute, but rather is reliant on domestic case law and common law and is designed in a manner that insufficiently addresses the need to protect human rights. Utilising Article 8 jurisprudence assists in understanding the gaps between the human rights safeguards established for comparable forms of police surveillance and biometric processing, and the lack of safeguards or oversight contained within the MPS governance. Understanding and applying jurisprudence using a doctrinal methodology is consequently well suited to the research aims of this thesis; namely, to understand the inadequacies and legal risks that are

[20] This thesis suggests this role is best addressed by the legislature as the elected arm of government, in light of the competing interests of the public policy objectives to use the technology and the protection of human rights. Legislation could also empower oversight bodies appropriately with powers to monitor the use of the surveillance. While police could tighten their governance further if they were minded to better protect human rights, the thesis suggests authorising legislation is preferable. The form of such tailored regulation is beyond the scope of this thesis.

demonstrated through the current MPS governance framework for LFR, and to demonstrate the legal standards and safeguards that should apply to regulate the lawful use of this form of surveillance.

There are three central claims this thesis makes using relevant ECtHR jurisprudence as a normative frame in arguing that the MPS deployment and governance model for LFR are at real risk of being in violation of Article 8. The first relates to the legal basis claimed by the MPS to support its use of LFR. The second relates to the breadth of discretion exercised by MPS decision makers at each stage of planning, approval and deployment of the technology. And the final claim relates to the proportionality of the purported benefits, and resultant rights impacts, of the use of this surveillance.

While there are other human rights that may be adversely impacted by the use of this form of surveillance, including protections against discrimination[21] and freedom of expression,[22] these are outside the scope of the current research project and will not be addressed here. They warrant further scholarship, including in respect of how these rights interact with the technology where biases exist and are perpetuated at scale, and how human oversight and control of the technology can be effected, particularly where police seek to use AI.

Contribution to Existing Literature

The focus of this thesis, and its contribution to the broader academic discourse on LFR use by police, is the governance model devised and utilised by the MPS. This analysis contributes to the broader discourse by highlighting the 'governance gaps' that permit the use of LFR in a manner that results in disproportionate and unjustified interferences with rights. Its contribution seeks to critically interrogate the governance framework to demonstrate the unlawfulness of the current model.

Extensive research has been undertaken into questions of lawfulness and human rights in relation to the use of FRT by police. This analysis includes an assessment of the

[21] *R (on application of Edward Bridges) v Chief Commissioner of South Wales Police* [2019] EWHC 2341, [201].

[22] *Glukhin v Russia*, (n 10), [57].

application of human rights law to LFR following the *Bridges* decisions,[23] socio-legal scholarship highlighting deficiencies in effective rights protections following the ongoing use of LFR by police in the UK,[24] sociological and regulatory considerations relating to LFR use by police,[25] and independent evaluation of the use of LFR by police and resultant human rights risks.[26] Non-government organisations ('NGOs')[27] and civil society organisations[28] have also published extensively on the topic of police use of LFR. This thesis contributes to the broader academic discourse by contending that self-regulation by police in using this form of rights-intrusive surveillance is both ineffective and perilous in light of the permissive and broad governance structure the MPS has developed to use LFR. The invocation of human rights legal terminology and concepts without effective protections or oversight that results in meaningful protections of rights is particularly pernicious coupled with the risks posed by LFR. Governments may believe that such technology is appropriately regulated by the police governance. The analysis presented in this thesis, and in the broader scholarship on the topic, contends that this is not the case, as the police have devised permissive self-regulatory mechanisms that permit too broad a range of circumstances in which the surveillance can be deployed.

This thesis contributes to broader scholarship and advocacy arguing for appropriate and tailored statutory controls to be implemented by Parliament to ensure LFR use by police

---

[23] Ni Loideain, Nora, Lawfulness and Police Use of Facial Recognition in the UK: Article 8 ECHR and *Bridges v South Wales Police* (April 5, 2023). Accepted for publication in R Matulionyte and M Zalnieriute (eds), Facial Recognition in the Modern State (Cambridge University Press 2024).

[24] Purshouse J and Campbell L, "Automated Facial Recognition and Policing: a Bridge Too Far?" (2022) 42 Legal Studies 209.

[25] Gentile, Giulia, Does Big Brother exist? Face Recognition Technology in the United Kingdom (January 20, 2023) <https://ssrn.com/abstract=4331633>.

[26] Pete Fussey and Daragh Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology (University of Essex, July 2019).

[27] Big Brother Watch, 'Face Off: the lawless growth of facial recognition in UK policing' (May 2018), <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> accessed 3 May 2023.

[28] Matthew Ryder QC, 'Independent legal review of the governance of biometric data in England and Wales' (2022, Ada Lovelace Institute) < https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf> accessed 3 May 2023.

is lawful, proportionate and only used where necessary to achieve a legitimate aim. It is particularly noteworthy in this respect that the House of Commons Committee on Science and Technology has called for a moratorium on the use of LFR by police until it is appropriately regulated by a dedicated statute that addresses oversight and accountability gaps in the current model, and stipulates the requisite thresholds for authorisation and use of LFR. [29] More recently, 65 members of the House of Commons and the House of Lords called for a moratorium of the use of FRT (in all forms) by police in the UK.[30] Worryingly, the MPS continues to utilise (and scale up)[31] its use of this technology in the absence of appropriately tailored statutory controls and oversight, to the detriment of effective rights protections.

[29] Science and Technology Committee, *The Work of the Biometric Commissioner and the Forensic Science Regulator* (HC 17 July 2019), [36] – [37].

[30] Jamie Grierson, 'MPs and peers call for 'immediate stop' to live facial recognition surveillance', The Guardian <https://www.theguardian.com/technology/2023/oct/06/mps-and-peers-call-for-immediate-stop-to-live-facial-recognition-surveillance> (accessed 6 October 2023).

[31] Matthew Weaver, 'Facial recognition could transform policing in same way as DNA, says Met chief', The Guardian, <https://www.theguardian.com/uk-news/2023/sep/11/facial-recognition-could-transform-policing-in-way-dna-testing-did-says-met-chief> (accessed 15 October 2023).

Chapter 1 | LFR Use by the MPS

FRT Forms and Uses

The MPS is responsible for providing policing services across 620 square miles of metropolitan London.[32] The MPS claims to have developed the foundational model for democratic policing in common law countries, valuing 'policing by consent' and emphasising the importance of police operating in a manner that strengthens the rule of law.[33] The MPS is also leading the use of LFR in the UK, utilising the NeoFace Watch system from global technology firm, NEC.[34]

FRT takes a number of forms and can be used in several ways by police. While the MPS uses three forms of FRT—all warranting human rights scrutiny—the scale of their use of LFR is significant compared with the other types of facial biometric technologies they use. During a typical deployment of LFR by the MPS, the biometric data of tens of thousands of people will be processed by the algorithm.[35] This form of FRT consequently warrants particular scrutiny with reference to human rights law, both as a result of the human rights impacts on individuals, and the impact on the enjoyment of privacy rights across communities where this technology is deployed.

LFR can be used either overtly or covertly, and it can be deployed using either dedicated cameras or as an overlay on existing camera systems (such as CCTV systems across public transport networks). LFR is used to identify individuals 'in real time' as they pass cameras that are connected to the facial recognition algorithm, analysing the live footage. The algorithm seeks to match individual biometric profiles of people passing the cameras against biometric profiles compiled on a 'watchlist'. Police will then intercept and

[32] Metropolitan Police Service, 'About the Met: Jurisdiction' (*Metropolitan Police Service*) <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/jurisdiction/> accessed 1 August 2022.

[33] Metropolitan Police Service, 'About the Met: The Met has a long and rich history to be proud of' (*Metropolitan Police Service*) <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/met-museums-archives/important-dates/> accessed 1 August 2022.

[34] NEC, 'NeoFace Watch: Protecting Your Community' (*NEC*) <https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html> accessed 1 August 2022.

[35] See, e.g., National Physical Laboratory, 'Equitability Study 2023', (n 18), 5.

arrest (if there are lawful grounds) the individual who has been identified by the algorithm. LFR is a form of AI that, if used by police, has the potential to significantly and disproportionately impact the human rights of a large number of people who may not be immediately aware that their biometrics have been processed.

The second form of FRT used by the MPS is retrospective facial recognition (RFR). RFR is used where an image or footage is held by police, and an algorithm processes biometric information from the footage against a database of other biometric profiles to find any potential matches. For example, police could use CCTV footage of a robbery where the assailant's face is visible and utilise RFR to check if the biometrics match any profiles from police custody photographs to identify the person.

Finally, operator instigated facial recognition (OFR) works by police taking a photograph of a person they have stopped (for example, a person they are searching) which is run against a database to check for a match (for example, to check the person's identity and whether they have any outstanding warrants for their arrest).

While all forms of FRT should be appropriately regulated and overseen in a manner that protects human rights, LFR presents the most significant rights impacts in the manner it is currently used by MPS and consequently is the focus of this thesis.

Operational Deployment and Authorisation of LFR

The MPS have published all governance documents and protocols they have developed to use LFR.[36] This is partially because of community concerns about police using this form of surveillance[37] and partially in response to the absence of specific authorising legislation underpinning its use.

The MPS deploys LFR by using dedicated cameras that are overlayed with a facial recognition algorithm. [38] As depicted in Diagram 1, the algorithm analyses the facial features

[36] Metropolitan Police Service, Advice and Information: Facial Recognition', (n 5).

[37] Matthew Ryder KC, 'Independent Legal Review Governance of Biometrics in England and Wales', (n 28).

[38] Metropolitan Police Service, 'Live Facial Recognition – Process Summary' (*Metropolitan Police Service*) < https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-process-summary-2023-web.pdf?__cf_chl_tk=9q.2Zcvy5w05xKt6dsxZwVdnSj_B4.ST.MDPBd4Jj98-

of individuals captured within the zone of recognition.[39] The algorithm compares mathematical calculations of the faces of people captured in live footage against the faces of individuals whose images have been uploaded to the watchlist.[40] If the two sets of biometric data match, then the algorithm issues an alert of the match to police.[41]

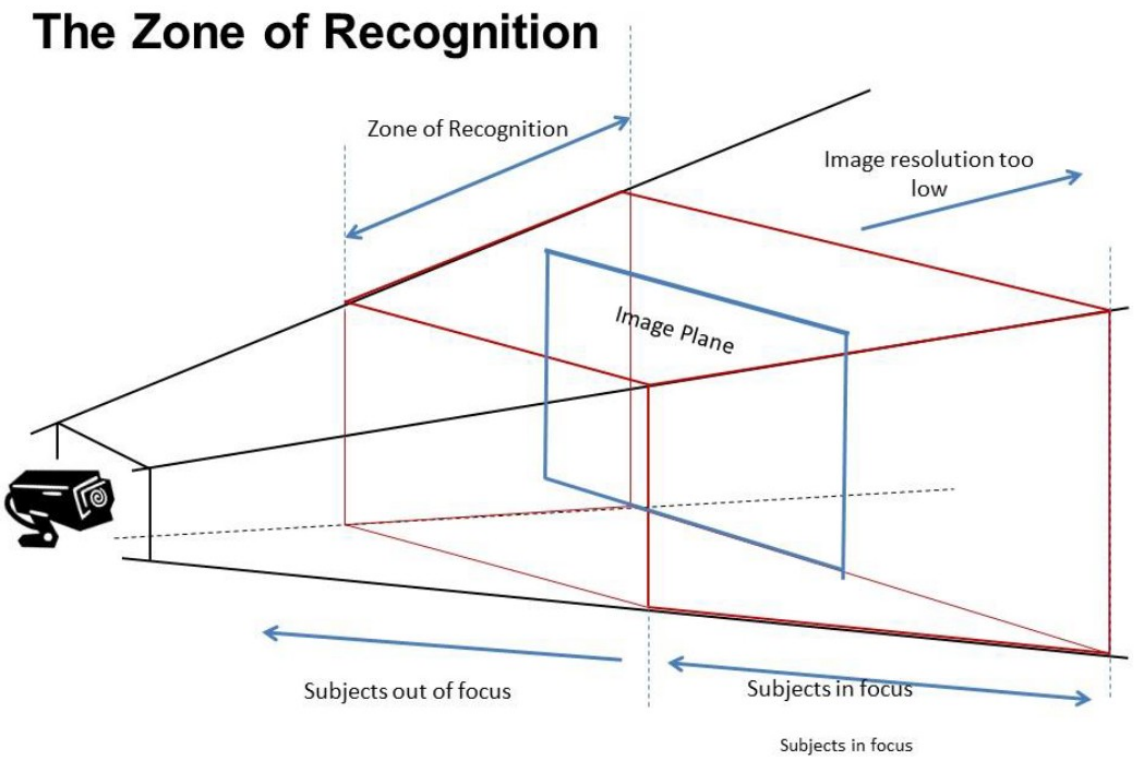


Diagram 1: Concept of zone of recognition from MPS governance[42]

During each LFR deployment (which typically span up to 12 hours) police surround the area where the cameras are deployed in order to apprehend any individual in the crowd who is identified by the algorithm.[43] An additional control is the role played by police analysts deployed within the van or control room. If the algorithm makes a match, an alert is made to

1690250774-0-gaNycGzNDeU> accessed 11 April 2023.

[39] ibid.

[40] National Physical Laboratory, 'Metropolitan Police Service Live Facial Recognition Trials' (Trial Period August 2016 – February 2019, Published February 2020) 9. <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf> Accessed 12 August 2022.

[41] Metropolitan Police Service, 'Live Facial Recognition – Process Summary', (n 38).

[42] National Physical Laboratory, 'MPS LFR Trials Evaluation 2016–2019', (n 40), [25].

[43] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

both the analyst and to police deployed among the crowd subjected to the surveillance. The analyst assesses whether they believe the person sought on the watchlist is the same person who has passed the cameras.[44] As depicted in Diagram 2, however, an alert will be made simultaneously to the analyst and police officer in the field.[45] Police who intercept the person will exercise their powers, including to ascertain the person's identity (and making an assessment as to whether they arrest the person, if this is warranted).[46] The police officer in the field is not bound to follow the confirmation or rejection of the match as assessed by the analyst in the van.

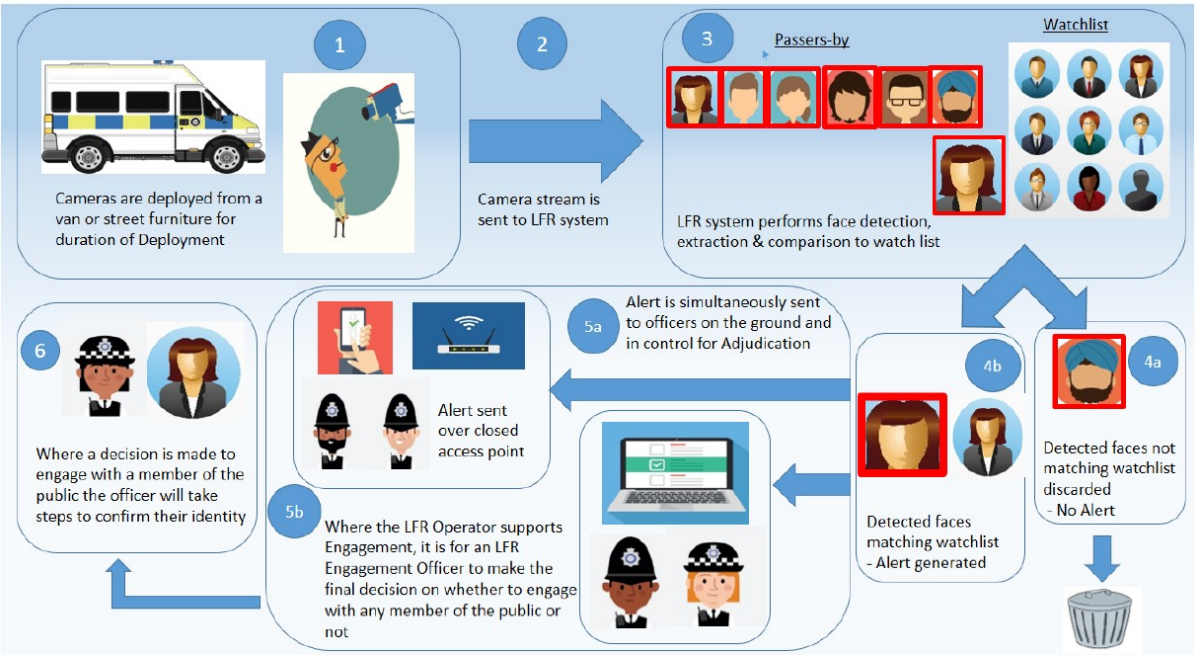


Diagram 2: The LFR process utilised by the MPS[47]

Each aspect of this process warrants human rights scrutiny: the reliance on common law and existing statutory powers by police to use this technology, the compilation of the watchlist, the authorisation of deployment locations, the thresholds set for offence types and other use cases (such as identifying witnesses and victims), the accuracy of the LFR

[44] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [21].

[45] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [21].

[46] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[47] National Physical Laboratory, 'MPS LFR Trials Evaluation 2016-2019', (n 40) [9].

algorithm in identifying biometrics in real time, and the efficacy of the human oversight and exercise of police powers where the algorithm alerts a match.

A critical analysis of each of these components reveals (arguably) that the MPS's use of LFR unlawfully interferes with Article 8 ECHR. The lack of clear legal authorisation for police to use this technology risks unlawfulness because:

a) it is insufficiently foreseeable and ineffectually protects against the arbitrary interference with the right
b) the lack of accuracy in relation to certain ethnic and gender identities risks the deployment not being found to be 'necessary to achieve a legitimate aim'
c) the watchlist compilation risks a disproportionate interference with the right (particularly with the breadth of categories for inclusion on the watchlist and the deployment location, and the lack of assessment of rights interferences for individuals proposed to be included on the watchlist to assess proportionality by the Authorised Officer [AO] before deployments).

The technology itself, including its procurement, the vendor and how the algorithm has been built (including the datasets that have been used to train the algorithm) also warrant human rights scrutiny.[48] These issues are beyond the scope of this thesis.

Overview of MPS Decision Makers

The MPS governance utilises three tiers of decision makers for the authorisation and use of LFR. At the top of this structure is the Gold Commander, at a minimum rank of Superintendent, who is the designated AO in the MPS governance documents.[49] The AO is responsible for the approval of the watchlist before each deployment.[50] The Gold Commander retains responsibility to ensure 'that the use of LFR remains lawful, necessary

[48] Office of the Biometrics and Surveillance Camera Commissioner, Commissioner for the Retention and Use of Biometric Material Annual Report January 2021 – March 2022 and Surveillance Camera Commissioner Annual Report March 2021 – March 2022 (report presented to Parliament pursuant to Section 21(4)(b) and Section 35(1)(b) of the Protection of Freedoms Act 2012), [134].

[49] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

[50] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

and proportionate' in light of the impacts on the human rights of individuals who pass through the zone of recognition.[51] As such, a significant degree of responsibility for human rights analysis and justification rests with this decision maker at each stage of the deployment of the technology.

The second-highest decision maker in this hierarchy is the Silver Commander, who is restricted to the rank of inspector or above. They hold the power to suspend or terminate the deployment of LFR at any time.[52] The Silver Commander is also tasked with ensuring the lawfulness, necessity and proportionality of the deployment, and is directed to have 'particular regard to the effectiveness of the safeguards in place whilst LFR is being used'.[53] The Bronze Commander is responsible for overseeing the police deployed 'on the ground' for the interception of any individuals identified by the system.[54]

Both the Gold and Silver Commanders have clear responsibilities in the MPS governance to identify and assess human rights impacts ahead of (and during) any LFR deployment.[55] It is less clear, however, what instructions or expectations the MPS have of the operational police and analysts deployed about relevant human rights considerations that should shape their use of the technology, and what training they are expected to undertake before using LFR that would appropriately acquit their responsibilities regarding human rights.

The analyst deployed within the van or control room is a key decision maker in MPS's use of LFR technology. This role purports to address the need for a 'human in the loop' as a key 'safeguard' against potential biases in the algorithm. In practice, however, the time available to the analyst to either confirm or reject the match made by the LFR algorithm suggests the quality and nature of this human intervention is limited as there are only a few seconds between an alert being made and the person passing out of reach of the deployed

[51] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

[52] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

[53] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

[54] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

[55] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [19].

police.[56] The resultant risk is that police are more likely to intercept a person where the algorithm has made a match, on the understanding they can release the person if the algorithm is later found to be incorrect.

Permissive Authorisation and Use of LFR

The MPS governance creates a tiered authorisation framework which suggests that human rights are appropriately considered and balanced at each stage of the use of LFR. However, in applying the relevant legal norms and safeguards to this model (as addressed in Chapter 3), it is apparent that the governance framework devised by the MPS does not achieve the right balance between the public policy objectives police contend support LFR use and the rights interferences resulting from its use.

The next chapter sets out the relevant Article 8 jurisprudence against which the MPS governance framework will be assessed in Chapter 3.

[56] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [10.8].

The MPS uses LFR to process the biometric profiles of all people who pass through the areas under camera surveillance connected to the algorithm. This will engage a wide variety of human rights, including the right to respect for private and family life (herein the 'right to privacy'), protection from discrimination, right to liberty and freedom of movement.

This chapter outlines the relevant jurisprudence relating to Article 8 that applies to the use of LFR by police. Of particular importance for this thesis is the jurisprudence that sets out the legal standards that must be met by the MPS for it to establish that its use of LFR amounts to a lawful interference with Article 8. There are three elements to this assessment: whether the interference with Article 8 is lawful, pursues a legitimate aim and is necessary in a democratic society.

In assessing whether the interference is lawful, the ECtHR does not require a bespoke statutory framework to govern the police use of LFR[57] but instead would assess whether the legal framework in place is sufficiently foreseeable[58] and protects against arbitrary interference with the right.[59]

With respect to addressing the requirement that the interference is necessary to achieve a legitimate aim,[60] the ECtHR would likely be satisfied that this is met considering the operational objectives of police in using LFR.[61] Finally, if the MPS's use of LFR were considered by the ECtHR, it would determine whether this use was necessary in a democratic society, which includes an assessment of the proportionality of the use of the technology in light of its impacts on Article 8.[62]

[57] *Barthold v Germany*, ECtHR 25 March 1985, 8734/79.

[58] *Sunday Times v the United Kingdom*, ECtHR 26 April 1979, 6538/74, [49].

[59] *Herczegfalvy v Austria*, ECtHR 24 September 1992, 10533/83, [91].

[60] *Merabishvili v Georgia*, ECtHR (GC) 28 November 2017, 72508/13, [295] – [296].

[61] These include: in the interests of national security, public safety, for the prevention of disorder or crime, for the protection of the rights and freedoms of others: Art 8(2) European Convention on Human Rights.

[62] *Sunday Times v the United Kingdom*, (n 58), [62].

Two relevant judgements of the ECtHR are summarised, *Gaughran*[63] and *Glukhin.*[64] They are set out with a particular focus on how the ECtHR may assess whether the use of LFR by MPS is lawful, pursues a legitimate aim and is necessary in a democratic society.

In *Gaughran*, the ECtHR noted the impact that the retention and subsequent processing of facial biometric data by police has on Article 8, and the corollary burden that arises for contracting states to establish any justifiable interference with the right where this type of processing occurs. The judgement is important in its assessment of the impact of retention of biometric data through custody photographs in light of the developing technologies available to police such as FRT. The case assists in guiding the assessment of proportionality of LFR use, particularly where retention and use of facial biometric data relates to lower-level offences (i.e., where such uses amount to a disproportionate limitation of the right in light of the offence at issue).

In *Glukhin*, the ECtHR considered the safeguards required for police use of this form of surveillance. The Court concluded that police had utilised FRT to identify the plaintiff (using RFR) and to arrest him (using LFR). The lack of appropriate safeguards, including the fact that police were apparently able to use the technology to investigate a minor administrative offence resulted in a disproportionate interference with the applicant's Article 8 right.

Both judgements elucidate relevant legal principles and thresholds against which there are significant gaps with the purported safeguards and legal grounds on which the MPS uses LFR. The *Gaughran* judgement prompts significant questions as to whether the legal basis upon which images are used by the MPS (including custody images) are sufficient; while the *Glukhin* decision prompts questions as to whether the technology is necessary in a democratic society, including where LFR is used to identify individuals wanted for summary offences, as witnesses or as victims of crime; and whether appropriate safeguards are in place to prevent disproportionate rights impacts.

[63] *Gaughran v UK*, (n 9).

[64] *Glukhin v Russia,* (n 10).

Article 8 ECtHR Jurisprudence: Overview

The MPS governance purports to apply legal standards in the authorisation and deployment processes for LFR, including human rights law. Further analysis of this justification is undertaken in Chapter 3. While 'human rights legal terminology' is invoked in this governance, Article 8 jurisprudence (as summarised in this chapter) suggests a significant gap exists between the MPS invocations of rights and the operational use of LFR that adversely impacts Article 8 rights.

As a preliminary point, Article 8 jurisprudence permits a wide margin of appreciation within which governments are able to utilise surveillance technologies in pursuit of achieving legitimate objectives.[65] However, it is also important to recognise that the rights protected under the ECHR are not static, and will develop and strengthen in response to the novel risks posed by digital surveillance. The further development of legal safeguards in light of technological and societal changes is reflected in the ECtHR's use of the living instrument doctrine, including in respect of Article 8.[66] The Court has repeatedly held that the ECHR is a 'living instrument … which must be interpreted in light of present-day conditions.'[67]

Summary of Article 8: Sequential Elements to Assess Lawfulness of LFR

Contracting States can limit Article 8 if their actions are lawful, achieve a legitimate aim and are necessary in a democratic society (including an assessment of proportionality). The law relating to Article 8 limitations is well established in ECtHR jurisprudence.[68]

---

[65] See, e.g., *Big Brother Watch and Ors v UK* App nos 58170/13, 62322/14 and 24960/15 (Grand Chamber 25 May 2021).

[66] See, e.g., *Pavlov and others v Russia* App no 31612/09 (ECHR 11 October 2022).

[67] *Tyrer v United Kingdom* App no 5856/72 (ECHR 25 April 1978) [31]. See also the Dissenting Opinion of Judges De Gaetano, Yudkivska and Grozev in *López Ribalda and others v Spain* (ECHR Grand Chamber 17 October 2019) in which they stated (at [2]), 'This case demonstrates the growing influence and control that technology has in our world, and more particularly, the collection and use of our personal data in our everyday activities. As a living instrument, the Convention, and therefore the Court, not only needs to recognise the influence of modern technologies, but also has to develop more adequate legal safeguards to secure respect for the private life of individuals.'

[68] *S & Marper v UK* App no 30562/04 and 30566/04 (Grand Chamber, 4 December 2008), [66].

States that seek to utilise innovative technologies (such as LFR) have an additional responsibility to ensure safeguards put in place adequately protect Article 8. The ECtHR stated in the *S & Marper v UK* judgement that:

> [T]he protection afforded by art.8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests … any state claiming a pioneering role in the development of new technologies bears special responsibility for striking the right balance in this regard.[69]

It falls to the MPS to demonstrate that the governance they have devised appropriately balances the impact on rights against the benefits offered by the use of the technology.

As a preliminary point, recent ECtHR jurisprudence has tended towards the Court assessing the lawfulness and proportionality requirements of Article 8 together, as opposed to distinct sequential elements for the state to establish in contending the interference is lawful. The analysis and application of relevant Article 8 jurisprudence is presented in Chapter 3 as distinct aspects (i.e., the 'lawfulness' requirement, followed by the 'legitimate aim' requirement, followed by an assessment of whether it is necessary in a democratic society). However, the ECtHR would likely address these aspects together in any determination it made following a judicial consideration of the lawfulness of the MPS's use of LFR.[70]

Article 8: Scope of the Right

The right to respect for private and family life protects a range of aspects essential to the ability of an individual to live the life they choose to live within their community. This includes

[69] ibid [112].

[70] See e.g. *Gaughran v UK*, (n 9), [70]; *Glukhin v Russia*, (n 10), [73].

protection of their bodily autonomy and integrity, their family and home, their correspondence and informational privacy.[71]

The protections offered under Article 8, particularly as they relate to 'private life', are 'not susceptible to exhaustive definition.'[72] The protection of private life embraces 'multiple aspects of the person's physical and social identity', which includes 'the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world.'[73] Consequently, the right is relevant in protecting the privacy of people in certain public spaces and interactions, with the ECtHR accepting this to include 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[74]

The proliferation of digital technologies has led to widespread personal data collection, and the range of algorithms that can build sophisticated profiles about the most sensitive and private aspects of individuals' private lives has led some to suggest that the concept of privacy in our society no longer exists.[75] This is, arguably, a self-serving claim made largely by technology companies seeking to facilitate the proliferation of surveillance technologies that do not comply with human rights legal standards and thresholds. Rather than leading to the end of privacy, the proliferation of technology has highlighted its importance in everyday life. Privacy should be understood as being engaged at various points on a spectrum.[76] The more significant the adverse impacts on an individual's privacy, autonomy, family and correspondence connected to the use of surveillance technology, the more relevant the right to privacy will become.

Privacy extends to protect the 'personal autonomy of every individual', as a fundamental foundation to liberty enjoyed in a 'free polity', with the ECtHR noting that any

[71] *S & Marper v UK*, (n 68) [103].

[72] *Glukhin v Russia,* (n 10), [64]; *S and Marper v UK,* (n 68), [66].

[73] ibid.

[74] ibid; *Lopez Ribalda and Others v Spain*, (n 67), [87] – [88].

[75] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' *The Guardian* (London, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 11 April 2023.

[76] Neil Richards, *Why Privacy Matters* (1st edn, Oxford University Press 2021), 2.

interference with this necessitates an 'objective justification' to be lawful.[77] While this has been established as a threshold for interference with Article 8, there are also well-established boundaries to the scope of protection offered by this right. Article 8 is qualified by understanding the level of seriousness in terms of the adverse impacts on the right and, second, whether the rights holder enjoyed a 'reasonable expectation of privacy' in the circumstances.[78] Courts have also accepted that the right may be limited in light of 'the scope of the justifications available to the state pursuant to Article 8(2).[79] While it might be assumed that a person moving through a public space where LFR is deployed by the MPS, such as outside a shopping centre or a busy train station, would have 'little to no expectation of privacy' for the purposes of this analysis, it is important to also note that the type of impact on privacy resulting from a person being subjected to this form of surveillance is different in important respects from mere observance in public places by others. A person's expectation of privacy may not be full anonymity when moving through a space where they can be observed by others, but this does not mean their expectations of privacy would also be limited such that they would accept that the state or police would identify them and their movements with precision if identified by the LFR system, including the processing of private and sensitive biometric data alongside other datasets held by police.[80]

It is also important to note that this form of surveillance is currently used by police overtly, which differentiates the scope of the protections offered by the right from its enjoyment in other contexts such as in the home.[81] While the 'expectations of privacy' are an important factor in assessing the application of Article 8 to LFR use, the ECtHR has accepted that the protection of private and family life can extend to public spaces.[82]

The protection offered by Article 8 is not all encompassing. As an example, the House of Lords found that Article 8 is not adversely impacted to the requisite standard of

[77] *Bridges v South Wales Police,* (HC), (n 21), [48].

[78] *R (Wood) v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, [17].

[79] Ibid, [22].

[80] *Glukhin v Russia*, (n 10), [76].

[81] *R (Catt) v Commissioner of Police of the Metropolis*, (n 14), [26].

[82] *Glukhin v Russia,* (n 10), [64].

seriousness in the context of searches 'the kind to which passengers uncomplainingly submit at airports.'[83] The expectation of privacy in a given circumstance is an important element that informs Article 8 interferences.[84]

This is also a salient example of where the proliferation of surveillance in the community may result in a reduction of the protection offered by the right to privacy. Put another way, the Courts may find the increased use of facial recognition technology by police results in a reduced 'expectation of privacy' if this use is widely accepted by the community. An example of this is evident in the community acceptance of biometric 'e-gates' used in major UK airports in place of human immigration checks.[85]

Gaughran and *Glukhin*

The following two recent judgements of the ECtHR provide helpful guidance as to what safeguards the Court expects contracting states to have in place for biometric processing to be undertaken in compliance with Article 8 requirements.[86] Both judgements are particularly important in assessing the adverse impacts posed by the technology and whether such impacts result in a disproportionate interference with Article 8 in light of the operational objectives that the MPS seeks to achieve.

Gaughran v UK

The *Gaughran* judgement related to the retention and use of sensitive biometric data, including fingerprints and DNA, for individuals who had been convicted of specified crimes.[87] Mr Gaughran had been convicted of drink driving, made to pay a fine and lost his driver's licence for 12 months.[88] As part of the criminal investigation and proceedings, the Police Service of Northern Ireland (PSNI) took records of Mr Gaughran's DNA, fingerprints and a

[83] *Gillan v Commissioner of Police*, (n 15) [28].

[84] Ibid, [28].

[85] Gwyn Topham, 'March of the robots: how biometric tech could kill off paper passports' (4 February 2023, The Guardian) < https://www.theguardian.com/politics/2023/feb/03/biometric-technology-paper-passports-redundant> accessed 11 May 2023.

[86] *Gaughran v UK*, (n 9), [70]; *Glukhin v Russia,* (n 10), [73].

[87] *Gaughran v UK,* (n 9), [3].

[88] ibid [7].

facial photograph taken while he was in police custody.[89] Mr Gaughran wrote to the PSNI requesting this sensitive data be deleted after his conviction had been spent (five years after the offence).[90] While the PSNI did remove his DNA profile from the national DNA database, it retained records of his DNA, fingerprints and the photographs taken during his time in custody on its own databases.[91]

The UK Supreme Court, in considering the matter before it was appealed to ECtHR, found that the retention of Mr Gaughran's biometric data by the PSNI was proportionate, partially because the applicant's photograph was stored on a stand-alone database that was not connected to any form of further processing (such as a facial recognition algorithm)[92] and partially because the legislated scheme in place was proportionate in determining that only individuals who had been found guilty of 'recordable offences' would have such data retained by authorities.[93] The Supreme Court noted that the margin of appreciation in state practice relating to the retention of biometric data by authorities had grown significantly across contracting states since the *S & Marper v UK* decision.[94] This suggested the interference with Mr Gaughran's rights was lawful and proportionate overall.

Mr Gaughran then brought an application before the ECtHR, alleging that the indefinite retention of his DNA profile, fingerprints and custody photograms in according with the PSNI blanket retention of personal data of anyone convicted of a recordable offences amounted to a disproportionate interference with his Article 8 right, and could not be justified.[95]

The ECtHR found that the retention of Mr Gaughran's DNA and fingerprint data amounted to an interference with his Article 8 right[96] and that the retention of his custody

[89] ibid [6].

[90] ibid [8].

[91] ibid [9].

[92] ibid [13].

[93] ibid [14].

[94] ibid [15].

[95] ibid [3].

[96] ibid [63].

photograph also amounted to an interference.[97] The latter conclusion is important in the context of assessing the MPS governance relating to LFR, as the ECtHR found the retention of the photograph by the PSNI amounted to an interference with Article 8—a conclusion that had not been reached in earlier cases on the subject of retention of photographs by the authorities.[98] The ECtHR came to this conclusion in light of current and emerging technological capabilities being adopted by police that allow additional processing of photographs in a manner that interferes with Article 8 rights (i.e., through the processing of facial biometrics in photographs by FRT).[99]

Another conclusion reached by the ECtHR which assists the analysis in Chapter 3 is that:

> [t]he Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.[100]

In Mr Gaughran's case, the PSNI only stored his custody images on their system, but the ECtHR noted that the PSNI system was connected to national databases which could be subjected to further data processing and searches using FRT.[101] Even though the photographic database storing Mr Gaughran's records was not connected to FRT at the time of the decision, the ECtHR found the connection with national databases where facial recognition was used amounted to an interference with his Article 8 right.[102]

The ECtHR then turned to the question of whether there was a lawful interference per Article 8(2). It found there was a sufficient legal basis for the police action in retaining the biometric data following Mr Gaughran's arrest and prosecution[103] and found that it was in

[97] ibid [64].

[98] ibid [65].

[99] ibid [65].

[100] ibid [66]; citing *S & Marper v UK,* (n 68), [67].

[101] *Gaughran v UK*, (n 9), [68].

[102] ibid [70].

[103] ibid [73].

pursuit of a legitimate aim (being the detection and prevention of crime).[104] The central focus of the Court's analysis in the judgement was consequently whether the retention of the biometric data was necessary in a democratic society, including whether it was proportionate.[105]

The ECtHR considered the margin of appreciation afforded to the UK in determining that biometric data would be retained indefinitely where specified offences resulted in successful convictions. Of relevance to the MPS LFR case study, although the Court found that many contracting states retained photographs and fingerprints for extensive periods (including for life), the 'rapid technological advances in this domain in particular concerning technology for facial recognition and facial mapping' could change the conclusion that such retention falls within the margin of appreciation if such technologies were used on these datasets.[106]

The ECtHR found the retention of sensitive personal information, including facial biometrics, was not proportionate in light of these technological developments. While not explicitly put, it appears that the Court recognised the significant difference between processing facial biometrics using manual (i.e., human) processes and the computational power offered by AI-driven algorithms such as those used by LFR.[107] This is important in contrasting the authority cited by the MPS (noted above) from *Catt*, where Lord Sumption concluded the capture of photographs by police presented no meaningful difference from the common law powers of a constable to observe people in public places in undertaking their duties.[108] Ultimately, the ECtHR held that the UK had 'overstepped' its margin of appreciation and that the retention at issue constituted a violation of Mr Gaughran's right to respect for private and family life.[109]

[104] ibid [75].

[105] ibid [76].

[106] ibid [80].

[107] ibid [86].

[108] *R (Catt) v Commissioner of Police*, (n 14), [26].

[109] *Gaughran v UK,* (n 9), [97]-[98].

The *Gaughran* judgement provides helpful guidance in establishing that retention and possible use of sensitive biometric data requires appropriate safeguards to be in place for the interference to be lawful, pursue a legitimate aim and to be necessary in a democratic society. While the retention periods are not comparable between the indefinite period proposed to retain Mr Gaughran's biometric data, and the LFR model deployed by the MPS (where biometric footage is retained for up to 31 days depending on the classification of the data by police), the impact on rights is made clear in the decision, and reveals the disproportionate impact on rights in light of the 'law enforcement' objectives claimed by the PSNI. It is important to note that the source of photographs used to create the watchlist is often custody images held by the MPS and obtained in comparable circumstances to the PSNI custody images database considered by the ECtHR in the *Gaughran* decision.

Furthermore, the nature of the offence that Mr Gaughran was prosecuted for (driving while intoxicated,) meant that the interference with his Article 8 right was disproportionate. This is significant because the MPS governance permits comparably 'minor' offences to be included in the compilation of watchlists.

Glukhin v Russia

Glukhin was the first judgement rendered by the ECtHR on FRT use by police. While the circumstances involving the applicant, Mr Glukhin, differ in some respects from the use of LFR by the MPS, the similarities between both use cases suggest a significant risk of the MPS model being found to be an unjustified interference with Article 8 rights should such a claim be brought in the future.

The case involved Moscow Police using FRT to identify and track Mr Glukhin after he had carried a cardboard cut-out of a dissident on the Metro as a form of protest.[110] Police were able to identify Mr Glukhin, who was previously unknown to them, using facial recognition algorithms run over CCTV footage from the Metro.[111] The police linked data

[110] *Glukhin v Russia,* (n 10), [68].

[111] ibid [68].

obtained from multiple sources (including social media) to identify, track and eventually detain Mr Glukhin.[112]

FRT algorithms are capable of processing large volumes of sensitive personal data, including biometric profiles, at near-instantaneous speeds, which has a more significant impact on Article 8 than would be the case if human operators were to track an individual's movements over a CCTV network. In this case, police received live notifications when Mr Glukhin's biometric profile was next identified entering the Metro system, and they dispatched police to intercept and arrest him.[113] While police would be able to identify and track Mr Glukhin without FRT, the resources required (utilising police analysts to monitor CCTV continuously across busy transport hubs until he next caught the train) to do this would likely limit police surveillance of this kind being reserved for only the most serious of offences.

Moscow Police utilised several forms of FRT, including LFR and RFR. Mr Glukhin's posts on the social media platform Telegram were identified by an 'anti-extremism' police taskforce, after which they obtained relevant CCTV footage of the time period within which Mr Glukhin travelled on the Moscow Metro and identified him using RFR.[114] Mr Glukhin stated in the proceedings that police informed him upon his initial arrest that he had been identified after police used facial recognition cameras on the Metro.[115] He was arrested at an underground station, suggesting the form of facial recognition was LFR (although this was never confirmed by Russia in its response to the case).[116]

Mr Glukhin initially challenged the actions of the police in Russian courts. He challenged the use of this form of surveillance for the investigation of 'administrative' offences such as the offence he was charged with, arguing that this level of offence did not permit the use of the powers relied upon by Moscow Police to utilise FRT. His domestic

[112] ibid [68].

[113] ibid [68].

[114] ibid [10].

[115] ibid [12].

[116] ibid [12].

challenge was unsuccessful and he thereafter submitted an application to the ECtHR, alleging *inter alia* a violation of Article 8.[117]

In his application before the ECtHR, Mr Glukin argued that the administrative offence proceedings violated his rights to freedom of expression and assembly under Article 10 ECHR, as well as his right to respect for private and family life under Article 8 ECHR. The latter claim concerned the processing of his sensitive biometric data in the context of police investigating the administrative (low level) offence.[118] The ECtHR cited the Russian Constitutional Court as having previously established that the powers relied upon by police to undertake a search using FRT (more particularly, 'audio and video-recording, photography, filming and other technical means [being used] during operational-search activities')[119] related to 'criminal offences' and not administrative offences such as the offence that Mr Glukhin had been charged with.[120] The Court found that the administrative classification of the charge laid against Mr Glukhin could not 'serve as the legal basis for the measures taken in the present case'.[121]

The ECtHR also canvassed 'relevant international material' in its judgement.[122] While not incorporating this into its eventual findings relating to the interference with Mr Glukhin's Article 8 right, it is still notable in giving an indication of the risks and contours of possible lawful use of FRT by contracting states. For example, the ECtHR referred to relevant guidance published by the United Nations (UN) High Commissioner for Human Rights in a report entitled 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests.'[123] This guidance elucidated how FRT can impact the enjoyment of a range of rights, including privacy, freedom of expression

[117] ibid [17].

[118] ibid [58].

[119] ibid [22].

[120] ibid [24].

[121] ibid [80].

[122] ibid [35] – [39].

[123] ibid [35].

and peaceful assembly. This is especially true if effective safeguards are not in place when such technologies are used.[124] The cited UN guidance stated that

> [r]ecording, analysing and retaining someone's facial images without her or his consent [constitutes an] interference with a person's right to privacy. By deploying facial recognition technology at assemblies, these interferences occur on a mass and indiscriminate scale, as this requires the collection and processing of facial images of all persons captured by the camera equipped with or connected to a facial recognition technology system.[125]

While these were not the exact circumstances in which Mr Glukhin had been identified, the UN guidance recognised the impact of FRT (particularly LFR) in interfering with a person's right to privacy 'on a mass and indiscriminate scale'.[126] This is directly relevant to the MPS governance model underpinning LFR use (as further explored in Chapter 3).

While not forming part of the decision relating to Mr Glukhin's circumstances, as he had been directly identified using FRT following the image of his protest being disseminated through Telegram, the ECtHR also referred to guidelines produced by the European Data Protection Board which stated:

> 36. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. *The process constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit* …[127]

[124] ibid [35].

[125] ibid [35].

[126] ibid [35].

[127] ibid [39] (emphasis added).

The ECtHR also extracted a report from a Russian human rights media project documenting the likely use of what amounts to both RFR and LFR by Russian police,[128] and that Russian authorities were likely reticent to explicitly acknowledge their use of FRT in any form 'because it is in the "grey zone" of Russian legislation'.[129] The ECtHR noted that Russia had not responded to specific questions as to whether it had utilised FRT in any form as part of the police investigation into Mr Glukhin and accepted that this presented 'difficulty' for Mr Glukhin in proving his allegation that the technology was used.[130]

The ECtHR accepted that the particular circumstances of the case (including the rapid identification of Mr Glukhin within a two-day period from the Telegram post being assessed by police to his arrest and the fact that no other identifying features aside from his facial biometrics were apparently available to police as part of the investigation) meant FRT was used by the Moscow Police.[131] The Court further concluded that this use (both in initially identifying him using the Telegram photographs, and then in identifying his location when he subsequently used the Moscow Metro) amounted to an interference with his right to respect for his private life protected by Article 8(1).[132]

The ECtHR then assessed whether this interference was justifiable in light of Article 8(2). As a preliminary point, the Court stated that 'questions of lawfulness and of the existence of a legitimate aim cannot be dissociated from the question of whether the interference was "necessary in a democratic society"'.[133] As already noted, if the ECtHR were to assess the use of LFR by the MPS, it is likely that the Court would consider the proportionality overall of the interference with Article 8 alongside questions as to whether there is a sufficient legal basis supporting its use and the interference was necessary in pursuit of a legitimate aim.

[128] ibid [40].

[129] ibid [40].

[130] ibid [69].

[131] ibid [72].

[132] ibid [73].

[133] ibid [78].

In *Glukhin*, the ECtHR found the use of FRT by Moscow Police amounted to an unjustified interference with Mr Glukhin's Article 8 right, alongside his freedom of expression protected by Article 10.[134]

The judgement reinforced the well-established, safeguards relating to Article 8 and surveillance, by emphasising the importance of clear and detailed rules to govern the operation and oversight of surveillance that impacts on personal privacy, including rules that govern:

> the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[135]

The *Glukhin* judgement shows the factors that will be considered by the ECtHR in assessing whether the use of FRT amounts to a justifiable interference with Article 8. The judgement gives an indication of the types of safeguards and permitted uses of FRT operating in a Contracting State to the ECHR and the circumstances in which the use of this form of surveillance will amount to a violation of Article 8.

Applying Article 8 Jurisprudence to the Use of LFR by the MPS

The summary of relevant jurisprudence presented here is important in demonstrating the difference between legal standards for lawful interferences with Article 8 and the insufficient safeguards established by the MPS to use the technology. This is the focus of Chapter 3, which is structured to assess the MPS governance in light of ECtHR jurisprudence.

The first stage would require the ECtHR to assess whether LFR interferes with the right to privacy of an affected person.[136] The Court would then consider whether there is a

[134] ibid [91].

[135] *Glukhin v Russia*, (n 10) [77]; *S & Marper v UK,* (n 68) [99]; *P.N. v Germany* App no 74440/17 (ECHR 11 June 2020), [62].

[136] *S & Marper v UK*, (n 68), [59].

lawful basis upon which the public authority can rely for the interference.[137] This includes consideration of whether there was a sufficient legal basis upon which the action or measure was undertaken, whether the action or measure was in compliance with the rule of law and whether the quality of the law was sufficient (including whether the law allowed for 'foreseeability' and protection from arbitrary interference with the right).[138]

This would be followed by an assessment of whether the use of the technology was in pursuit of a legitimate aim (being one of the aims enumerated in Article 8(2)). An area of potential unlawful interference with Article 8 arising from this analysis arises from the accuracy of the algorithm that underpins LFR, which also engages Article 14 of the ECHR alongside domestic equality and non-discrimination laws.[139] If the technology is inaccurate in matching wanted persons to the live footage captured, then it would likely fall foul of this requirement.

The final step in the legal analysis would require the ECtHR to consider whether the interference is necessary in a democratic society. This would require the Court to balance the interests of the Contracting State in achieving its public policy objectives against the protection of Article 8 rights of the affected individuals. The Contracting State must demonstrate that its actions seek to achieve a 'pressing social need,' as opposed to the interference being justified as 'useful, reasonable or desirable' only.[140] The ECtHR would also assess whether the measure adopted is the least impactful on rights available to the public authority.[141] This analysis would also address the existence (or otherwise) of the judicial oversight and authorisation process of the interference, and the adequacy of parliamentary oversight and authorisation, both as relevant safeguards to ensure any interference with Article 8 is justified.[142] Collectively, this fourth stage entails a 'proportionality' assessment of the interference, assessing the adverse impacts on the right

[137] ibid, [95].

[138] ibid, [95].

[139] *Bridges v South Wales Police* (EWCA), (n 13), [201].

[140] *Roman Zakharov v Russia* App no 47143/06 (Grand Chamber, 4 December 2015), [232].

[141] ibid [260].

[142] ibid [234].

to privacy of the affected person against the achievement of the legitimate aim underpinning the operational use of LFR by the MPS.[143]

Each aspect of the analysis could result in a finding that the interference is unjustifiable and a violation of Article 8 has occurred.

The final chapter applies this legal analysis in assessing the adequacy of the MPS governance in protecting human rights. The resultant analysis, finding significant gaps between expected safeguards and the adverse impacts on the right to privacy from the use of LFR, demonstrates the need for appropriate regulation and oversight of police use of this technology.

[143] *S & Marper v UK*, (n 68), [101].

Chapter 3 | Application of Article 8 Safeguards to the MPS's Use of LFR

This chapter begins by addressing whether and how Article 8 is engaged by the MPS's use of LFR. Drawing on the MPS deployment model, it is clear that there are a number of interferences with Article 8 resulting from their surveillance.[144] Interferences extend to individuals placed on the MPS watchlist, individuals whose biometric information is processed as they walk through the zone of recognition, individuals who are stopped by police as a result of a match being made by the system, and additional impacts on rights where such a match is incorrect (i.e., where police detain a person based on an incorrect match being made by the algorithm alone where they would otherwise not have formed the requisite suspicion of the person).[145]

While the MPS deployment model is used overtly and in public spaces, which might suggest the scope of the right to respect for private and family life is limited in its application, Article 8 is still engaged by its use.[146]

Having established that LFR interferes with Article 8(1), the chapter then turns to Article 8(2), utilising the ECtHR jurisprudence summarised in Chapter 2 to critically analyse the MPS governance and operational use of LFR. This commences with an examination of whether the MPS have a sufficiently clear and accessible legal foundation upon which they can use LFR. The legal basis claimed by the MPS to utilise LFR technology relies partially on existing common law powers and provisions of the Police and Criminal Evidence Act 1984 ('PACE'), alongside an apparent reliance on 'consent' from the public in having their biometric profiles processed as they pass through the zone of recognition. The MPS governance also relies upon the decisions from the UK High Court and Court of Appeal in *Bridges* as authority for the proposition that police use of LFR is lawfully authorised by the common law. Both decisions are set out in this chapter in order to assess the

[144] This thesis does not address admissibility issues which could arise, including the requirement of a 'significant disadvantage' being experienced by the applicant. The focus provided here instead is on the analysis of a claim on the merits.

[145] Metropolitan Police Service, 'Live Facial Recognition – Process Summary', (n 38).

[146] *Wood v Commissioner of Police*, (n 78), [17].

appropriateness of the MPS relying on these decisions in this way. The overall contention provided here is that the sources relied upon by the MPS are insufficient to address the lawfulness requirement in Article 8(2). If it were accepted by the ECtHR that the MPS does not have an adequate legal basis to use LFR, then its continued use (by definition) would amount to an unlawful interference with the right.

The next aspect to consider is whether the MPS's use of LFR technology is in pursuit of a legitimate aim. The broad law enforcement objectives set out in Article 8(2) would likely support the police use of LFR. However, the analysis presented here suggests that the inaccuracy of the algorithm underpinning LFR (particularly in relation to women of colour) undermines the argument from the MPS that the use of the technology achieves a legitimate aim (arising from its inaccuracy in identifying wanted individuals of some ethnicities and gender identities).

The final analysis presented in the chapter seeks to answer whether the use of the technology is necessary in a democratic society, including a proportionality assessment. It is here that the clearest legal risk of invalidity arises with the MPS deployment model, as the broadly permissive watchlist categories, the permissive deployment governance, and the ineffectual oversight and authorisation processes result in insufficient safeguards and disproportionate limitations on Article 8 and the enjoyment of other human rights protected under the ECHR.

The chapter concludes that appropriate regulation (likely through a tailored statute to govern the use of LFR by police) should be implemented to address the significant gaps identified through the critical analysis outlined in Chapter 3 and to ensure safeguards are in place for police use of LFR.

Interference with Article 8(1)

LFR engages privacy as it is a form of surveillance. It also engages privacy as a form of biometric identification. As with other forms of biometric identification (such as police use of fingerprints or DNA), the impact of LFR on privacy can be understood as a significant

interference with this right and its protection of an individual's right to their identity and autonomy.[147] The intersection between emerging technologies and privacy is a topic that frequently comes before the ECtHR, which has noted the importance of rigorous evaluation of emerging surveillance technologies in order to ensure they are consistent with human rights law.[148]

The nature of the harms experienced by individuals subject to this form of biometrics processing is contested, particularly between police who minimise the impacts on rights stemming from the use of LFR[149] and human rights advocates who warn of both the existing and potential impacts on rights that result from the proliferation of this form of surveillance in society.[150]

As summarised in Chapter 1, police use of LFR will adversely affect Article 8 in several ways. This includes the rights of people passing through the zone of recognition,[151] and individuals whose biometric data is uploaded to the watchlist.[152] The MPS governance suggests its conception of rights limitations is more limited than this.

MPS justify the lawful use of LFR on the basis that, for the majority of people, the technology will involve a momentary rights impact where the system processes their facial biometrics, followed by the automatic deletion of their biometric data if no match is made between their biometrics and the biometric data on the watchlist.[153] On this basis, LFR presents a marginal impact on human rights including Article 8. This was the rationale of the Court of Appeal in *Bridges*, which noted in relation to the assessment of the extent of the limitation of Article 8 by the police use of LFR that the 'overwhelming majority of cases' where individuals' biometrics were processed resulted in no match being made, meaning the

[147] *Gaughran v UK,* (n 9), [70].

[148] *Big Brother Watch v UK*, (n 65), [311].

[149] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[150] Big Brother Watch, 'Face Off: FRT in UK', (n 27).

[151] *Glukhin v Russia*, (n 10), [39], citing a report from the UN Office of the High Commissioner Human Rights in *obiter*.

[152] Ibid, [39], citing a report from the UN Office of the High Commissioner Human Rights in *obiter*.

[153] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

biometric profiles were ‘immediately and automatically deleted’ and the underlying footage would be subsequently destroyed 31 days after being captured.[154]

The analysis presented in this thesis, however, suggests that the risks posed by the technology to Article 8 are more significant than this equation suggests. For example, if police were to link the biometric profiles obtained by LFR with other datasets, such as those containing the biometric profiles and identification information connected to driver’s licences and passports, then the impact on Article 8 would be manifestly more significant than what is outlined by the MPS in their justification to use the technology.[155]

Linking these datasets would mean that law enforcement could identify individuals as they moved through spaces surveilled by LFR, with significant adverse impacts on their privacy and other human rights. These human rights impacts are not theoretical, as demonstrated by the judgement of the ECtHR in *Glukhin*.[156] While the current parameters set by the MPS governance would not permit the linking of large datasets in this way, it is of note that there is nothing currently preventing the police from using the technology like this. Moreover, recent calls made by the police minister suggested this outcome is desirable (i.e., linking the biometric data stored as part of the UK passport system with FRT in order for police to identify shoplifters).[157] Reports from NGOs and legal advocates in December 2023 indicated that the UK Government intends on amending legislation to allow police to uitlise biometric data stored through the driver’s licences database, giving them access to the biometric data of 50 million people across the UK.[158]

---

[154] *Bridges v SWP* (EWCA), (n 13) [17].

[155] Human Rights Watch, ‘China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App’ (1 May 2019) <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass> accessed 1 August 2022.

[156] *Glukhin v Russia*, (n 10) [68].

[157] Aletha Adu and Rajeev Syal, ‘UK passport images database could be used to catch shoplifters’, The Guardian, <https://www.theguardian.com/uk-news/2023/oct/02/uk-passport-images-database-could-be-used-to-catch-shoplifters>, (accessed 20 October 2023).

[158] Daniel Boffey, ‘Police to be able to run face recognition searches on 50m driving licence holders’, The Guardian, <https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-searches-on-50m-driving-licence-holders>, (accessed 21 December 2023).

The MPS's use of LFR has differentiated impacts on privacy rights. For each person who passes through the zone of recognition and has their biometrics processed (of which there may be many thousands over each hour the technology is deployed) there will be adverse human rights impacts. The ECtHR has noted that such impacts engage Article 8, even where no further processing or adverse impacts arise (such as where no matches are made and where the unmatched biometric profiles are automatically deleted by the algorithm).[159] Adverse impacts are more readily evident for individuals whose biometric profiles are used on the watchlists, and also where matches are made resulting in further rights intrusions following the exercise of police powers. An instructive contrast is seen in the experience of Mr Bridges, where his sensitive biometric data was captured, processed and deleted,[160] and Mr Glukhin, whose sensitive biometric data was captured, processed and then used to create live alerts to notify police of his movements such that he could be tracked down and arrested.[161]

Accepting that Article 8 is engaged, and interfered with, by the use of LFR, any judicial challenge to the MPS model would turn to whether the interference is in accordance with the law. The burden would be on the State to establish that each of the three requirements was met. The following analysis suggests that the use of LFR by MPS is not in accordance with the requirements of Article 8(2) and consequently violates Article 8.

Article 8(2): Lawful interference

Understanding the lawful basis upon which the MPS use LFR is the first area from which potential unlawfulness is apparent. Without a sufficient legal basis upon which LFR use can be established, the interference with Article 8 will likely be found to be unlawful if judicially challenged. The proceeding analysis suggests that the MPS's justification for LFR use is insufficient and ineffective to authorise its use in all use case circumstances outlined in the MPS governance.

[159] *Glukhin v Russia*, (n 10) [39], citing a report from the UN Office of the High Commissioner Human Rights in *obiter*.

[160] *Bridges v SWP* (EWHC), (n 21), [52].

[161] *Glukhin v Russia*, (n 10), [8] – [14].

The MPS have devised a range of governance documents and assessments in purporting to use LFR lawfully. These include an equality impact assessment for the purposes of addressing the requirements of the Public Sector Equality Duty ('PSED'), a data impact assessment for the purposes of the General Data Protection Regulation ('GDPR'), and frequent references to lawfulness, proportionality and necessity with reference to both the Human Rights Act 1998 and the ECHR.[162] Each of these documents provides some insight into how the MPS use LFR. A critical analysis of the accuracy of these documents, and whether they address the legal obligations on MPS in relation to each legal framework (i.e., the Equality Act 2010, GDPR), is beyond the scope of this thesis. There remains, however, many questions as to the nature and quality of protections for rights that result from this governance.

While the governance documents appear to reference the relevant legal obligations and terms appropriately in outlining the use of LFR, the safeguards that would be expected to give effect to the intended protections of each legal framework are ineffectual.

As per the summary of relevant jurisprudence in Chapter 2, the MPS must establish that its legal authority to use LFR addresses the requirement to protect individuals from arbitrary interferences of Article 8, and that the legal basis is sufficiently foreseeable. The MPS seek to address this requirement through a governance document entitled 'Legal mandate'.[163] This document warrants particular scrutiny as LFR is a form of biometric processing that is not regulated by dedicated statute in the UK, unlike other forms of biometric identification used by police such as fingerprint processing[164] and DNA.[165] In their utilisation of LFR, the MPS relies on existing statutory powers relating to the capture and processing of photographs alongside common law powers.

The legal mandate for the MPS to deploy LFR are the common law powers that police exercise in their day-to-day duties, alongside s 64A of the PACE, as the lawful

[162] Metropolitan Police Service, Advice and Information: Facial Recognition', (n 5).

[163] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[164] Police and Criminal Evidence Act 1984 (PACE), section 61.

[165] PACE, section 63.

authority.[166] The MPS reference a schematic (see Diagram 3) throughout its governance documents that outlines its claimed legal authority.

The diagram suggests overlapping layers of regulation and oversight of the use of LFR. At the centre is PACE and policing common law powers. Both of these 'sources of legal authority' relied on by the MPS will be assessed as to whether they sufficiently address the lawfulness requirement summarised in the Chapter 2 outline of relevant Article 8 jurisprudence.

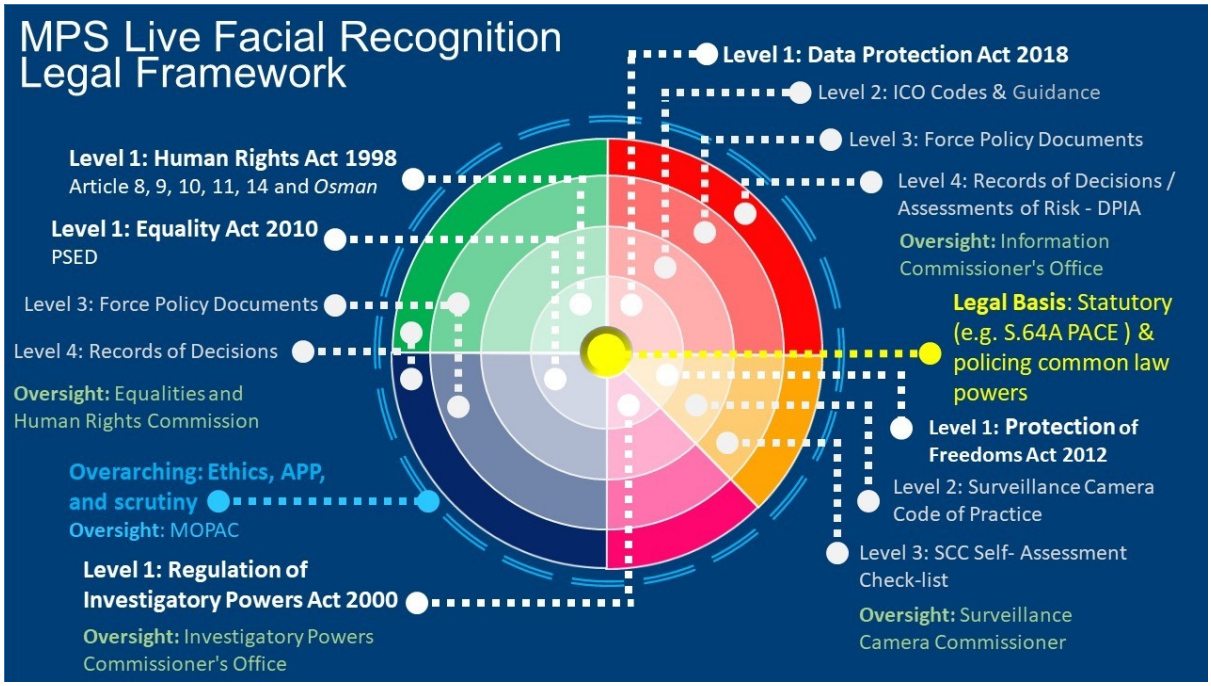


Diagram 3: Legal authority diagram: MPS governance[167]

Police and Criminal Evidence Act

PACE provides the statutory authority for a wide range of police powers. Section 64A, which the MPS cite throughout their legal mandate document, permits the 'Photographing of suspects etc', including a number of circumstances in which police have a lawful power to take a person's photograph if the person is under arrest, taken into custody, given a penalty notice or subject to police action listed in the section (such as where a person is given a

[166] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[167] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

direction under s. 35 of the Anti-social Behaviour, Crime and Policing Act 2014).[168] The MPS specifically cite s. 64A(4)(a) of PACE, which relates to a photograph held by police that has been obtained under this section being used or disclosed for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.[169] The MPS cites this section as the legal basis for the creation and use of the LFR watchlist, drawing on custody photographs.[170]

This may authorise the use of the technology on individuals who are wanted as part of police investigations into crimes, or who are subject to outstanding warrants or have absconded from lawful custody. But it remains unclear (and arguably beyond the scope of PACE) for this provision to justify the impacts on human rights of all other individuals whose biometrics are processed when they pass the deployed cameras and who are not in any way connected to the justifications highlighted in the section above. Additionally, it is unclear how s. 64A justifies the use of photographs included on the watchlist of individuals sought by police on welfare grounds or individuals wanted by police as witnesses to crimes that police are currently investigating. Nor is it clear s. 64A authorises the use of photographs obtained by police from other sources (such as social media) for watchlist use.[171] The categories of wanted persons for inclusion on the watchlist are analysed in greater detail in relation to the proportionality assessment below. The extract of PACE at the heart of the legal schematic that the MPS uses to justify LFR is consequently ill-suited to the manner in which the technology works, particularly in light of the impacts on human rights and privacy of all people whose biometrics are processed as they pass the cameras.

Furthermore, construing PACE in this very broad way may result in the exercise of police powers in a manner that arbitrarily interferes with Article 8. Police appear to use confined statutory powers in a broad manner that goes beyond what the Act authorises. Arbitrary interferences extend to the inclusion on watchlists of witnesses and victims of

[168] PACE, section 64A(1B)(ca).

[169] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[170] Metropolitan Police Service, 'LFR: Legal Mandate', (n 3).

[171] Metropolitan Police Service, 'Standard Operating Procedures', (n 8).

crime, and individuals who 'may pose a risk to themselves or others'.[172] This will be addressed further in relation to proportionality.

The common law powers that the MPS contends support their use of LFR include the powers to protect life and property, preserve order and prevent threats to public security, prevent and detect crime, bring offenders to justice and uphold national security.[23] As with the reference to PACE, this is a very broad range of potential justifications to ground the lawfulness of LFR. It does not specifically document how LFR is lawfully authorised in the manner used by the MPS in light of the interference with Article 8 and other human rights.

The MPS states that the legal schematic (and associated legal obligations and frameworks that apply to police) is appropriate to rely upon in this circumstance by analogising the use of the technology to the ability for any individual police officer to identify a wanted person in a crowd of people, but to do this more effectively than any individual officer would be able to and at a more significant scale.[173] However the scale and nature of Article 8 interferences posed by LFR is not considered by this analogy. Unlike an individual police officer, LFR can identify and track thousands of people through their sensitive biometric data, and process and store this information in a manner that is not comparable to the ability of a single—or indeed, many—police to replicate. The Article 8 interferences are manifestly more significant due to the scale and processing power available to the algorithm in undertaking this form of surveillance.

The common law powers of police are broad in their construction, and exercised to achieve operational objectives that align with the stated objectives in Article 8(2), including for the detection and prevention of crime, and for public safety.[174] Consequently, it is likely that some use cases, such as those involving the identification of individuals wanted for serious offending, would find sufficient lawful authority from these sources of power.

[172] ibid.

[173] Metropolitan Police Service, 'LFR: Legal Mandate', (n 4).

[174] Metropolitan Police Service, 'Standard Operating Procedures', (n 8).

The common law powers of police do not extend to the capture and processing of photographs and video of any person for any reason,[175] which results in legal risk for some LFR use cases set in the MPS governance. Officers do not have a power (either statutory or at common law), to compel a person to have their photograph taken, although there is a power that can be authorised by an Inspector to force a person to remove anything that conceals their identity.[176] Therefore, there are real risks of unlawful capture and processing of photographs, including sensitive biometric data, particularly where individuals are unaware that police are not empowered to compel them to have their images processed by LFR. The MPS governance does instruct officers to this point, directing that they cannot force a person to pass through the zone of recognition of an LFR system unless the threshold for arrest is reached in relation to an individual (at which point the power under PACE may be available to them).[177]

The legal basis of the MPS governance is insufficiently precise to justify or authorise all aspects of the LFR deployment model, including the foreseeability requirements. This has implications for the lawfulness claims made by MPS in the legal mandate document.

The legal mandate is silent on what basis the MPS relies on to lawfully process all biometric data of the crowds of people passing through the zone of recognition, including the majority of individuals passing the cameras who will not be suspected of having committed any crimes or of being of any interest to police. The legal justifications in the MPS governance are focused on the use and processing of biometrics relating to the watchlist.[178] The only legal basis relied upon for the former impacts on Article 8 are the common law power of police to observe people in public.[179] No justification is provided in the legal mandate in relation to the capture and processing of biometrics of people who pass the zone of recognition with no match being made, apparently as police believe any such impacts on

[175] *Bridges v Chief Commissioner of South Wales Police* [2019] EWHC 2341, [85] – [89].

[176] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[177] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[178] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[179] *Catt v Commissioner of Police,* (n 14), [26].

rights is marginal as sensitive biometric data is automatically deleted in these circumstances.[180]

While it was not a matter that the ECtHR had to determine in the *Glukhin* decision, it is relevant to note that the Court included material from the UN Office of the High Commissioner for Human Rights that stated momentary processing of biometrics through LFR limits the right to privacy.[181] While this is not yet settled law, it is arguable that the MPS must demonstrate a lawful justification for the interference with Article 8 rights of all people who pass through the zone of recognition, rather than only for those whose biometrics are matched to someone on the watchlist.

***Bridges v South Wales Police*: Lawful Authority for LFR?**

The legal mandate of the MPS cites the High Court and Court of Appeal decisions in *Bridges v South Wales Police* (SWP) as authority for its lawful use of LFR. The appropriateness of these decisions being relied upon by the MPS to support its use of LFR is therefore assessed.

SWP utilises LFR in a manner substantially similar to that used by the MPS.[182] Dedicated CCTV camera systems attached to police vehicles are deployed to pre-approved locations, and police are placed throughout the crowds subjected to the surveillance so they can apprehend any individual identified by the LFR algorithm.[183] The SWP's use of LFR was challenged by Mr Bridges, who was supported by the NGO, Liberty.[184] Mr Bridges claimed that his rights (including Article 8) were unlawfully interfered with when his biometrics were processed during two deployments of LFR.[185] The UK High Court noted the established jurisprudence on Article 8 that states privacy covers the 'physical and psychological integrity

[180] *Bridges v SWP* (EWHC), (n 21), [59].

[181] *Glukhin v Russia*, (n 10) [39].

[182] South Wales Police, Police Heddlu De Cymru, 'Facial Recognition Technology' (South Wales Police) <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/> accessed 1 August 2022.

[183] ibid.

[184] *Bridges v SWP* (EWHC), (n 21) [8].

[185] ibid [10].

of a person'.[186] The Court also acknowledged that the right covered many aspects of the person's identity, including their 'gender, name, other means of personal identification and of linking to a family, ethnic identity, and elements relating to a person's right to their image'.[187] LFR directly impacts a number of these aspects of a person's identity, particularly where biometrics are matched with personal information on the watchlist and this information is then disseminated among the police deployed as part of the LFR operation.

The SWP suggested that because their use of LFR was overt (using dedicated cameras rather than existing CCTV networks and ensuring sufficient notices were posted before a person entered the field of vision of the cameras such that they could avoid having their biometrics processed by the cameras if they chose by walking around them) and only deployed in public places, it did not engage or limit Article 8.[188] The High Court disagreed, noting that a person's expectations of privacy were an important (but not determinative) factor in assessing whether and to what extent Article 8 was engaged.[189] While the High Court acknowledged that the capture of CCTV footage alone (particularly where its impact was comparable to a person being observed by another person in a public place) would have a marginal impact on the right to privacy, it also concluded that the processing or the creation of a permanent record of this footage would more significantly impact Article 8.[190]

The High Court further accepted that Article 8 was engaged, even where biometrics were captured, stored and processed only momentarily (i.e., where no match was made between the individual's biometric profile and those on the watchlist).[191] The High Court found that, although his Article 8 rights were interfered with, the interference was marginal.[192] As Mr Bridges was not on the watchlist devised for use by the SWP, the High Court noted his biometrics were instantly deleted by the system, with no further resulting interferences

[186] ibid [47].

[187] ibid [47].

[188] ibid [51].

[189] ibid [54].

[190] ibid [54], citing *PG and J.H. v UK* App no 44787/98 (ECHR 25 September 2001) [57].

[191] ibid [57]-[59].

[192] ibid [62].

with his privacy.[193] Thus, no violation of Article 8 was found. Mr Bridges appealed the decision to the Court of Appeal.

The Court of Appeal decision found the LFR model utilised by the SWP (which mirrors that used by the MPS in many aspects) allowed too broad a discretion to satisfy the requirements of Article 8, particularly the 'who' question relating to the formulation of watchlists[194] and the governance on the location for deployments (the 'where' question).[195] The Court of Appeal stated that its decision was limited to the facts before it, rather than assessing the lawfulness and proportionality of the use of LFR by police as a whole.[196] Critically, the Court noted that its decision should not be taken as the legal foundation for the ongoing use of LFR by police in the UK:

> We do not accept that, in the present case, it is either necessary or helpful to consider hypothetical scenarios which may arise in the future … We consider that what must be examined is the particular interference with Article 8 rights which has arisen in this present case and in particular whether that interference is in accordance with the law. Whether other uses of police power in other contexts will be lawful in the future will be a matter to be considered if the facts of such a case arise in practice. This is consistent with the approach of the European Court of Human Rights, which usually asks whether there has been a violation of an applicant's rights on the particular facts of the case before it.[197]

The MPS legal mandate cites both decisions in stating that existing police powers, stemming from the office of constable, provide sufficient lawful powers to use the technology.[198] This appears to contradict the Court of Appeal judgment, which stated its

[193] ibid [59].

[194] *Bridges v SWP* (EWCA), (n 13) [91].

[195] ibid [91].

[196] ibid [60].

[197] ibid [60].

[198] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

decision should *not* be taken as a blanket lawful authority by which law enforcement could use the technology.[199] Further scrutiny as to the existence and scope of the legal basis for police use of LFR is warranted.

Legal Authority: 'Consent'

The MPS governance appears to supplement the broad and ill-fitting legal authorities listed in their legal mandate document that MPS claim support its use of LFR by predicating the operation of LFR on the consent of individuals whose biometrics are processed.[200] As a preliminary point, it is important to note that the information commissioner has found (in their guidance to police across the UK on the lawful use of LFR) that consent is an insufficient legal basis to justify its use.[201]

One basis on which MPS claim to obtain consent in using LFR is the signage requirements established in the LFR governance. Clear public signage is erected before the zone of recognition to 'allow them [individuals] sufficient time to exercise their right not to walk into the Zone of Recognition,'[202] and all LFR use requires published notification ahead of the deployment (such as through the MPS social media accounts) and on the day (i.e., by police handing out pamphlets explaining the technology and the process that occurs if a person passes through the cameras).[203] Officers are instructed that any person who is seen to avoid the cameras is not, in and of itself, committing any offence or warranting further investigation by police.[204]

[199] *Bridges v SWP* (EWCA), (n 13) [91].

[200] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

[201] Information Commissioner's Office, Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, (Official Paper, 31 October 2019, Reference 2019/01), 10 – 11.

[202] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7).

[203] Ibid.

[204] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).



Diagram 4: Public notices of LFR use by MPS in London, July 2022[205]

As is shown in Diagram 4, the signs erected around LFR deployments include QR codes that link users to the MPS website containing all governance and evaluation documents relating to LFR use.[206] Technically, this allows an individual the opportunity to ascertain the application and interference with their rights before they walk through the zone of recognition and their biometric data is processed by the system.

However, as with other aspects of the governance framework that the MPS have devised for their use of LFR, these 'protections' are superficial. If a person avoids having their biometrics processed by LFR, they may attract police attention and be detained while police seek to establish their identity and reason for avoiding the system.[207] The alternative is

[205] Twitter – Zack Polanski, 15 July 2022, accessed 1 August 2022, <https://twitter.com/ZackPolanski/status/1547598987665977348/photo/2>.

[206] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[207] Footage of an LFR deployment by MPS captured in this BBC clip documents a man's detention and questioning after he 'puts up his hoodie' to avoid having his face captured by the LFR cameras: BBC Click, 'Fines

to proceed through the zone of recognition on the expectation that they will not be identified by the system and that the impact on their rights will be momentary. However, this process does not allow for meaningful consent from affected persons. To obtain meaningful consent, individuals would need the ability to not have their biometrics processed and to avoid any further consequences such as police intervention. It would also require individuals to be properly informed of the nature of the surveillance and its impacts on human rights if they consented to having their biometrics processed in this way.

This summary of the legal framework that MPS utilises to justify its use of LFR gives an indication of the common issues stemming from the model they have devised. Broad claims of legality are made across the governance, with frequent invocations of human rights terms throughout. But the notable absence of any legal safeguards or categories beyond which it would be unlawful for the MPS to use this technology result in a wholly permissible legal governance structure that places little meaningful oversight or regulation on the use of this surveillance by police across London. While the publication of the legal mandate addresses the accessibility requirement of the 'legality assessment', its content is unclear as to the legal authority for some use cases (particularly those involving minor offences or no offences at all, as in the case of victims of or witnesses to crime). Furthermore, the reference to PACE appears ill-equipped to support all LFR use cases, which arguably results in arbitrary interferences, such as those involving victims or witnesses to crime.

An additional area of potential unlawfulness is the MPS governance designed to guide authorisation decisions in the creation of watchlists and the authorisation of deployment locations. These two broad and permissive key aspects were the grounds on which the Court of Appeal found the SWP's use of LFR to be unlawful in *Bridges*. This means that the MPS must show that the legal basis for their use of LFR is sufficiently clear and available to individuals during the Article 8(2) analysis stage to avoid potential unlawfulness.

and Facial Recognition' (2019) < https://youtu.be/0oJqJkfTdAg> accessed 1 February 2023.

It is, consequently, important to assess the role of the AO as defined in the MPS governance. The AO is responsible for acquitting all the pre-deployment reports and being satisfied that all legal thresholds are reached before any LFR deployment is authorised.[208] The governance and operating procedures made publicly available by the MPS are principally directed to the AO for this purpose. This leaves the primary human rights burden on the AO's figurative shoulders, including determining who should be included on any watchlist used for the deployment and whether a proposed deployment should be authorised. However, the breadth of discretion exercised by the AO is too broad to meet the legal standard established in Article 8(2) jurisprudence for any interference with the right to be lawful.

The breadth of categories within which a person's biometric profile might be added to the watchlist also presents challenges to the foreseeability threshold required in Article 8(2). The threshold requires an individual to be able to foresee how the legal framework will apply in the context of interference with Article 8.[209] However, it is challenging to understand the circumstances in which the watchlist will be compiled, and this affects the foreseeability of the technology's application, as demonstrated with the discretion for compiling the watchlist outlined above. Although the MPS cannot be required to notify individuals who will be added to the watchlist, Article 8 jurisprudence indicates that there must be appropriate safeguards in place to ensure that rights are protected and that there is no disproportionate or unlawful interference.[210] This could include, for example, a minimum threshold of seriousness for an individual to be added to the watchlist, and a requirement for judicial oversight and approval before deployments of the watchlist itself.

During deployment, LFR cameras are positioned to maximise the number of facial profiles processed.[211] From a practical perspective, it is challenging for an individual to take the time to understand the LFR deployment while among a large crowd, before reaching the

[208] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7), 8.

[209] *Roman Zakharov v Russia*, (n 140), [244].

[210] *Big Brother Watch and Ors v UK*, (n 65) [348].

[211] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

zone of recognition and having their biometrics processed. Were a person to click through the QR code to the relevant MPS website containing the governance, and were they then able to navigate to the relevant thresholds for the authorisation and use of LFR, they would be presented with the challenge of understanding the thresholds for use (which, as has been explained in the context of protection from arbitrary interference with Article 8, are imprecise and broad).

Overall, the analysis presented here demonstrates that certain use cases of LFR meet the lawfulness requirements as summarised from the relevant jurisprudence in Chapter 2. The breadth of uses of LFR suggests that some risk of unlawfulness could be established, however, particularly in relation to the breadth of categories within which MPS can add individuals to the watchlist, and in relation to the adequacy of the legal authority for the processing of biometric data of individuals who are not wanted by police but whose data is processed by passing the cameras.

The next part of this chapter assesses whether the interference posed by the MPS' use of LFR technology furthers a legitimate aim.

Legitimate Aim

If it were satisfied that a sufficient legal basis existed for the MPS to use LFR, then the ECtHR would turn to whether the use of the technology was necessary to further a legitimate aim. This requires that the Contracting Party satisfy the Court that the interference furthers one of the legitimate aims listed in Article 8(2). This involves the state demonstrating the rational basis or connection to the legitimate aims specified in the ECHR, which relevantly in this case study include 'public safety', 'the prevention of disorder or crime', and 'the protection of the rights and freedoms of others'.[212]

One aspect of the MPS governance that may not meet this requirement is the direction to the AO as to whether a wanted person may be proximate to the deployed LFR cameras. On the question of whether the interference pursues a legitimate aim, the AO is

[212] European Convention on Human Rights, Article 8(2).

directed to consider whether the wanted person may be proximate to the LFR deployment.[213] The MPS governance directs the AO to consider this when deciding whether to authorise or refuse the proposed watchlist and deployment location. This appears to align with the legitimate aim requirement. However, further discretion is afforded to the AO to add individuals wanted for serious offences, including murder, rape, kidnap and grievous bodily harm, regardless of whether the police have any intelligence to suggest the person will be in the vicinity of the deployed cameras.[214] In other words, the AO is not required to consider whether a person will be in the vicinity of the camera if they are wanted by police for serious or indictable offences. There is reference to the AO ensuring such inclusion is 'necessary and proportionate' but this amounts to a hollow human rights protection in light of the open discretion left to the AO to determine this, and the absence of further instruction as to what human rights protective factors must be considered in their decision.

The MPS governance, which was analysed in the context of lawfulness above, also has relevance in addressing the rational basis or connection between the interference, which is the use of LFR, and the legitimate aim that the MPS seeks to achieve. For example, the wide discretion afforded to the AO to authorise the inclusion of certain categories of wanted persons, despite the MPS having no information or intelligence connecting the person to the place where LFR will be deployed, does not result in the requisite connection being established.

Additionally, the accuracy of the algorithm in identifying faces has a bearing on this outcome. Usually, the accuracy (or more particularly the biases within the tool) are considered in the context of equality and non-discrimination rights, including Article 14 of the ECHR, alongside the domestic Public Sector Equality Duty found in the *Equality Act 2010.*[215] Whilst this focus is justified considering the primary harm that results from the bias in the algorithm, such outcomes can also have a meaningful impact on the ability for police to argue their use of LFR has a rational connection to the achievement of a legitimate aim. If

[213] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[214] Ibid.

[215] *Bridges v SWP* (EWCA), (n 13) [201].

the tool does not accurately identify wanted individuals, then by definition it cannot be argued it is a necessary interference to achieve a legitimate aim. This would also be a relevant consideration in assessing the third aspect of Article 8(2) justification (whether it was necessary in a democratic society, including whether it was proportional to the rights impacts resulting from the use of the technology).

The accuracy of the watchlist depends on the currency and quality of the photographs used. The AO is also directed to consider the currency of images held by police for individuals who are proposed to be added to a watchlist. If images held are old or of poor quality, they may not be suitable to be included. This is due to the risk that they will not lead to an accurate match where LFR is deployed and such data may lead to incorrect matches.[216]

Assessing whether LFR is necessary to achieve a legitimate aim requires transparency in its operation and its outcomes. It may be more challenging for the State to demonstrate that its use of LFR is in pursuit of a legitimate aim If the tool is inaccurate in identifying wanted persons. Assessing the accuracy of the tool, however, is difficult for affected persons for a number of reasons.

Technology can facilitate or hinder the protection, promotion and fulfilment of human rights, but it is important to note that in many respects, technology by its design and use is 'biased against disclosure and accountability.'[217] Its inscrutability is partially attributable to its design and form, which requires a high level of technical literacy to scrutinise.[218]

The relationship between the private sector, which is predominantly responsible for creating these tools, and the governments that use them is often covered by commercial in confidence arrangements. This can hinder the transparency and accountability that would otherwise be expected of governments.[219] Furthermore, human rights law, both

[216] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[217] Molly K. Land and Jay D. Aronson, 'The Promise and Perils of Human Rights Technology' in Land and Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018), 10.

[218] Note that an expert witness called by Liberty, Dr Anil Jain, could not ascertain whether LFR was affected by bias due to commercial arrangements preventing scrutiny of the FRT algorithm: *Bridges v SWP* (HC), (n 5) [155].

[219] Ibid [14].

internationally and domestically, binds states and governments, but not non-state actors such as companies that create the tools.[220] This presents challenges for accountability, particularly where the functions, powers and responsibilities that would otherwise be accountable to an individual officer employed by the state to provide services are now provided through an algorithm procured from the private sector.

Indeed, it has been noted that unless obligated to do so, developers of AI tools will not voluntarily 'offer full explanations covering the process, justification for, and accuracy of algorithmic decision-making'.[221] This is partially a result of the complexity of the tools, which makes it difficult to provide transparency into how they work. The sensitivity of the data on which algorithms are built and the need to protect the intellectual property that underpins how the tool works also contribute to this issue.[222] These factors present significant challenges to understanding the operation of the LFR algorithm and whether it is sufficiently accurate to warrant its lawful use by police.

Scope of Legitimate Aim: Prevention of Disorder and Crime, Protection of the Rights and Freedoms of Others

One of the primary responsibilities of police is the prevention of crime and the promotion of public safety. The listed justifications for the MPS to use LFR broadly align with these responsibilities.

The MPS claims that, as an operational tool, LFR helps to identify and stop 'dangerous people who are wanted for serious criminal offences' and helps the MPS to 'keep Londoners safe.'[223] The breadth of potential categories within which individuals may be included on the watchlist, however, is wide and certainly extends beyond keeping Londoners safe by identifying and stopping 'dangerous people'.

At a strategic level, the MPS claim that the use of technology will:

[220] ibid [14].

[221] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in an Age of Big Data and AI' (2019) Colum Bus L Review 494, [503] – [504].

[222] ibid, [503] – [504].

[223] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7).

> enable the MPS to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities such as violent and other serious crime. LFR technology will increase intelligence-led enforcement opportunities including those relating to knife and gun crime, child sexual abuse, terrorism, and helping to safeguard vulnerable persons. It will also help to locate those wanted by the courts or in breach of their bail conditions.[224]

This long list covers almost all conceivable law enforcement and public safety responsibilities that MPS are entrusted with. It extends from addressing crime that poses the highest risk to the largest number of people, right through to identifying individuals who are at risk of being victims of crime, and everything in between.

At an operational level, the MPS contend that the overt use of LFR offers a range of policing benefits in identifying individuals in public places. This includes identifying individuals for arrest by police where they are wanted for criminal offences; preventing individuals from entering areas where they may cause harm (such as individuals who pose a threat to public events, and those who are subject to football banning orders); identifying individuals who may pose a risk of harm to themselves or others (stalkers, terrorists, missing persons); and supporting proactive policing operations designed to address instances of violent crime in particular places.[225]

Rational Connection to Legitimate Aim

The rational connection to achieving the legitimate aim can be assessed by the instructions and use of LFR by police, and through analysis of the accuracy and bias of the algorithm that underpins the technology.

The overt model of the MPS is an example of how the deployment model contains some weaknesses in its ability to establish a rational connection between interference and achieving a legitimate aim. The AO is directed, somewhat contradictorily, to the fact that

[224] Ibid.

[225] Ibid.

individuals who are wanted by police after committing criminal offences will likely change their movement patterns and locations frequently to evade police capture.[226] Consequently, it is unclear how the AO is to assess the likelihood that an individual will be geographically proximate to the proposed LFR deployment. Because police utilise LFR overtly and in a manner that purports to allow individuals to circumvent the technology, it is likely that wanted individuals will be able to avoid detection.

Similarly, the AO is directed to make decisions acknowledging that intelligence about a wanted person's movements may be redundant as the person seeks to evade police identification and capture by changing their movements and location. This in turn results in a 'hollow' human rights protection for the individual because the ambiguity and contradiction in the directions given to the AO do not provide a sufficiently clear state of mind that the decision maker must meet before authorising the inclusion of an individual on the watchlist.

Furthermore, the accuracy of the tool will have a determinative impact on the ability of MPS to claim a rational connection between the use of LFR and the pursuit or furtherance of the legitimate aims specified in Article 8(2), such as the prevention of disorder and crime.

The ECtHR has recognised that to combat the harm caused by crime, police must use 'modern scientific techniques', including LFR, for investigating and identifying crime.[227] However, the accuracy thresholds of the algorithm must be appropriately established such that the technology will achieve a legitimate aim. This necessitates consideration of the efficacy of the tool as it is used by the MPS.

Evaluation of Accuracy and Bias

The accuracy of the algorithm underpinning LFR warrants particular scrutiny in understanding whether the use of LFR achieves a legitimate aim.

The use of LFR by MPS has been evaluated on multiple occasions since it was first used. Earlier evaluation (including by the University of Essex) found significant discrepancies in the accuracy of the tool, particularly relating to the identification of individuals according to

[226] ibid [27] – [28].

[227] *Glukhin v Russia*, (n 10) [85].

their ethnicity and gender identity.[228] More recent evaluation has found higher rates of accuracy, suggesting the algorithm continues to 'improve' its ability to identify individuals of different ethnicities and gender identities than it was previously able to.[229] The accuracy of the technology is briefly summarised here to highlight the rational connection between the interference and the legitimate aim, whilst also acknowledging continued weaknesses that remain in the tool and the implications for this if police use the tool to identify individuals whose facial biometrics are not as accurately identified by the algorithm.

The constant evaluation and scrutiny of the accuracy of the LFR algorithm, and the identification and management of any biases that affect the tool, is a legal requirement the MPS must acquit. Indeed, as the information commissioner noted in relation to the use of LFR by police in the UK:

> [W]ithout clear evidence of effectiveness based on a thorough and transparent evaluation process, it is difficult to see how the strict necessity threshold could be reached or how the intrusion into individuals' rights and freedoms could be considered proportionate.[230]

The MPS have consequently undertaken internal evaluation of the tool using their own expertise,[231] and have also commissioned the National Physical Laboratory (NPL) to undertake an independent assessment of the accuracy of the algorithm they use.[232]

It is important to note the human rights impacts that even this assessment can pose, as an evaluation that is constructed in a certain way may suggest a high degree of accuracy from a statistical perspective but may still result in disproportionate and biased outcomes

[228] Pete Fussey and Daragh Murray, *Independent Report on MPS use of LFR*, (n 26), [117]; Thomas Brewster, 'London Police Facial Recognition 'Fails 80% of the Time and Must Stop Now'' *Forbes* (4 July 2019) <https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/?sh=75557c7ebf95> accessed 14 April 2023.

[229] National Physical Laboratory, 'Equitability Study 2023', (n 18).

[230] Information Commissioner's Office, *Information Commissioner's Opinion LFR* (n 202) [16].

[231] National Physical Laboratory, 'Equitability Study 2023', (n 18).

[232] Ibid.

that adversely impact the human rights of individuals detained on the basis of the tool. Put another way, the evaluation may show statistical accuracy in the operation of the algorithm, while masking the significant and unlawful biases that result from the use of the tool among certain cohorts of people. Even a small number of people who are unlawfully detained on the basis of the erroneous algorithmic outputs will result in unlawful limitations of Article 8. This is the case even where the numbers of people in this category are statistically insignificant in light of the overall number of processed biometric profiles.

As an example of this, the MPS assesses the accuracy of their tool partially on the metric of matches compared to false matches, and also on false matches as a ratio of all biometric profiles processed during a deployment.[233] This latter calculation is particularly concerning, as a deployment may involve the processing of tens of thousands of faces and a far smaller number of incorrect matches being made.[234] The tool may consequently appear to have a very high rate of accuracy, with its inaccuracy being calculated as a decimal fragment of one, but will still result in inaccurate and biased matches. Statistically, the tool's accuracy is almost perfect, with an insignificant error rate. However, the impact on human rights arising from this error is far more significant than the statistical analysis would suggest for the individuals who have been incorrectly identified by the tool and detained by police.

An alternative basis for calculating the accuracy and 'necessity' of the use of the tool has been put forward by the information commissioner, who rejected the basis for calculating the accuracy of the tool put by the MPS, and instead suggested that the tool should be assessed on a metric that had a more tangible community safety benefit.[235] This could entail assessing the tool based on the circumstances in which it led to an arrest, prosecution and conviction of a person for a serious offence. This would more clearly substantiate the community safety benefits of using the technology.[236]

[233] ibid [22].

[234] See e.g., evaluation of Notting Hill Carnival Deployment, National Physical Laboratory, 'MPS LFR Trials Evaluation 2016-2019', (n 18) [9].

[235] Information Commissioner's Office, *Information Commissioner's Opinion LFR* (n 202) [16] – [17].

[236] Information Commissioner's Office, *Information Commissioner's Opinion LFR* (n 202) [16] – [17].

The risk posed by inaccurate matches made by the algorithm leading to disproportionate and unjustified police interventions could also be addressed if oversight focuses on the baseline set for accuracy of the tool.[237] The accuracy of the LFR tool can be set by the user (i.e., the level of confidence with which the tool has matched a person's biometric profile captured through live camera footage compared to a biometric profile on the watchlist).[238] To ensure that LFR use remains lawful, pursues a legitimate aim and is necessary in a democratic society, it is imperative to ensure that accuracy levels are set to minimise or eliminate incorrect matches. However, setting the threshold at a higher level will also mean that some accurate matches (calculated with a lower rate of certainty) do not reach the threshold and consequently no alert will be made by the system.[239]

The MPS calculate the 'true recognition rate' and the 'false recognition rate', using 'blue faces' (i.e. MPS staff placed on the watchlist to check the correct functioning of the algorithm where LFR is deployed) to identify the true recognition rate (alongside any correct matches made between people wanted by police and people on the watchlist).[240] The false recognition rate threshold for deployment is one false match for every 1,000 people who pass the camera.[241] This calculation appears somewhat self-serving, in that, depending on the location, any single deployment may be expected to process tens of thousands of faces each hour.[242] It was estimated that the two LFR deployments involved in the *Bridges* case processed half a million faces, with the biometrics of any individual potentially processed multiple times as they passed the zone of recognition.[243] The scale of biometric profiles processed during an LFR deployment can mask the human rights impacts on the comparatively small number of false matches made by the system.

[237] Information Commissioner's Office, *Information Commissioner's Opinion LFR* (n 202) [17].

[238] National Physical Laboratory, 'Equitability Study 2023', (n 18) [5].

[239] ibid [5].

[240] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7).

[241] National Physical Laboratory, 'Equitability Study 2023', (n 18) [5].

[242] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7).

[243] *Bridges v SWP* (EWHC), (n 21) [36].

The accuracy of FRT is not static. Large-scale studies undertaken by the National Institute of Standards and Technology in the US, for example, found that between 2013 and 2018 the failure to match the correct image improved from 4% failure in 2014 to 0.2% failure by 2018, with a search database of 26.6 million biometric profiles. [244]

It is challenging to identify the biases that may affect the LFR system considering a policy position adopted by the MPS. All data captured by the deployment of the LFR is deleted within specified timeframes (for no match made, biometrics are deleted immediately, if a match is made, then biometrics are deleted after 31 days).[245] An additional overlay, however, is that the MPS does not capture the data of biometric profiles processed according to race, gender or any other protected characteristic on the watchlist as 'the routine retention of data relating to protected characteristics would mean the MPS holding and processing data in circumstances where it does not have a policing need to do so.'[246] There are prohibitions on the police and other government entities using or processing data that relates to protected characteristics under the Equality Act 2010. This impedes the ability to assess the accuracy of the tool according to race and gender in a manner that would otherwise identify racial or gender biases. These biases are visible to the community and are a component of the transparency that the MPS should bring to using this technology.[247]

Lowering the threshold for accuracy in LFR will result in increased matches to the biometric profiles on the watchlist, but will also result in higher rates of inaccuracy and biased matches.[248] The standard face-match threshold used by the MPS in their deployments resulted in a variation of true positive identifications for different demographic groups ranging from 83% to 93% accuracy. The variation mirrored differences for

[244] Natalia Menendez Gonzalez, 'Development or dystopia? An introduction to the accountability challenges of data processing FRT' (2021) 26 Communications Law 2, 89, [82].

[245] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[246] ibid.

[247] ibid.

[248] Nora Ni Loideain, 'Lawfulness and police use of LFR', (n 23) [19].

environmental effects, such as weather and lighting, which ranged from 83% to 94% accurate.[249]

This metric is of considerable value in the context of assessing the lawfulness, proportionality and necessity of the technology as deployed by the MPS. It marks the rate at which individuals are falsely matched by the algorithm, which (if it were reflective of real world deployments) would result in the wrongly identified person being stopped by police, questioned, and even fingerprinted, in order that the error were identified.

The accuracy of the tool varied in relation to this metric according to the threshold set for the face-match score. This is the calculation of the match made by the algorithm. The lower the score, the less likely it is that the tool has identified the correct individual with the biometric profile on the watchlist.

There were no recorded false positive identifications at a face-match score of 0.64; there was one false positive identification at a face-match score of 0.62; and there were seven false positive identifications at a face-match score of 0.60.[250] The NPL found a statistically significant imbalance (i.e., bias) in the rate of false positive identifications at a face-match score of between 0.58 and 0.56, with 'more Black subjects having a false positive than Asian or White subjects.'[251] This dynamic is important. The evaluation found that the operation of the algorithm was not statistically significant when the threshold for a match (the face-match score) was set high enough to require the algorithm to only make alerts when the compared biometric profiles between the live footage and the watchlist were a practically certain match. If this were reduced, then the algorithm's error rate would increase, and the inaccurate performance would be according to different demographic factors (i.e., ethnicity, age and gender). Rather than finding that the tool was free of these discriminatory biases, the NPL found that the accuracy settings could be set such that such errors were not manifested in the results.

[249] National Physical Laboratory, 'Equitability Study 2023', (n 18) [4].

[250] Ibid [5].

[251] Ibid [5].

The cost of this, however, is that the number of matches overall drops, as the algorithm will only issue alerts where there is a sufficiently high calculation of a match between the biometric profiles. As this is not independently overseen or regulated, the resulting risk is that the MPS may adjust the face-match score to identify more individuals who may be wanted, and will then assess whether the person identified is the wanted person. The MPS may adjust the rate lower than what the NPL found resulted in zero false positive identifications (0.64) because it reduces the alerts issued overall, which raises questions as to whether it is an effective use of police resources. For example, a busy deployment of 80,000 faces processed over a shift may result in five or six alerts. In light of their findings, the NPL recommends 'where operationally possible' that a face-match score of 0.6 or higher is used[252] but this is not a legislated requirement, and it remains within the discretion of the MPS to adjust this level as they see fit.

The LFR algorithm settings determine the accuracy of the matches. When NPL adjusted these settings it found that the tool made false positive alerts disproportionately for Black and Asian ethnicities, and for women.[253] The NPL evaluation found that differences in accuracy between ethnicity and gender were 'statistically insignificant' where the face-match threshold was set at 0.6, finding in particular that the tool was most accurate at identifying the Asian-Female group of study participants and least accurate at identifying the Black-Female group of study participants.[254] It is important to note the definition of 'equitable outcomes' used by the NPL for the purposes of this review is (understandably) framed in a statistical sense, meaning that 'differences, where any exist, in the outcomes for the subjects from different demographics should be [statistically] inconsequential.'[255] This is not the same meaning as would arise in the context of human rights law, whereby discriminatory outcomes leading to police powers being unjustifiably used on individuals because the tool inaccurately identifies different genders and ethnicities would likely result in a breach of

[252] ibid [5].

[253] ibid. [22].

[254] Ibid [4].

[255] ibid [24].

human rights and unlawfulness. As has already been noted, it is incumbent on MPS to address such inaccuracies before using the tool, particularly where discriminatory outcomes would otherwise result from its use.

The NPL evaluation only assessed the operation of the LFR algorithm used by the MPS rather than fully replicating their deployment model. After footage was captured at the five pilot sites in London and Cardiff, researchers processed it using the algorithm to assess whether any true positive or false positive matches were made.[256] Importantly, the researchers did not seek to analyse the impact that the human in the loop plays in the process. They deployed the algorithm as if it operated autonomously, whereas the process would usually make an alert which would need to be confirmed or rejected by the human in the loop (the police analyst deployed in the van monitoring the live footage and the watchlist images).[257] It consequently remains unclear what impact is made when human judgment is introduced into the process. It is unclear if errors made by the tool are identified and addressed before the incorrectly identified person is stopped by police, or whether human involvement is affected by 'confirmation bias' which could lead to false positive identifications being 'confirmed' by the human in the loop, resulting in an individual being stopped and questioned by police without justification.

Importantly, the NPL found that 'there is no fixed face-match threshold at which in all mated identification searches the correct reference is returned at Rank 1, and any non-mated identification search would return zero matches.'[258] Put another way, the NPL evaluation was unable to identify a threshold at which the tool was completely accurate in only identifying matches between those who were on the watchlist and those who passed the LFR cameras.

Inaccuracies in the operation of the system can result in unlawful interferences with Article 8 where the use of the technology is consequently not necessary to pursue a legitimate aim. Important aspects of the accuracy of the tool, and questions as to the

[256] Ibid [5].

[257] ibid [5].

[258] ibid [14].

appropriateness of directions given to the AO as to the currency of watchlist images and likelihood (or even possibility) of the wanted person being proximate to the deployment, result in some risk that a judicial challenge could conclude that the LFR model is not in pursuit of a legitimate aim.

The greatest legal risk remains with the third step of the analysis, being whether the interference is necessary in a democratic society.

Necessity, Proportionality and Fair Balance

Is the Interference Necessary in a Democratic Society?

The final aspect the ECtHR would consider regarding the lawfulness of interference with Article 8 is whether it is necessary in a democratic society. This includes an assessment of the proportionality of the interference in light of the impact on affected individuals' rights.

In assessing the overall proportionality of the MPS governance, the analysis presented in this chapter will assess the breadth of categories for watchlist inclusion and the inadequacy of the authorisation process undertaken by the AO (including that assessments are not conducted for each person proposed for inclusion on the watchlist); the location authorisation process; and the inadequacy of operational police as a human in the loop safeguard under the current model.

Assessing the proportionality of LFR includes several elements. The ECtHR would consider the nature and extent of the interference with Article 8, the importance of the purpose of the limitation and whether there are less restrictive options available to achieve the same objective.

Assessing the proportionality of LFR use overall, it is clear that there is a risk of the technology being used in a disproportionate way. The ubiquity of CCTV cameras combined with the ability of the algorithm to process large volumes of data could 'enable continuous surveillance of specific individuals' and 'mass surveillance on an unprecedented scale.'[259]

[259] EU Fundamental Rights Agency, *Preventing unlawful profiling today and in the future: a guide* (Research Paper, Luxembourg, 2018) [16].

The adverse impacts on human rights would be significant and arguably unlawful. Privacy, autonomy and liberty would all be severely curtailed. Such an impact would be clearly unjustified in a democratic society. The capacity of the facial recognition algorithm far exceeds the ability of police to identify and track a person using CCTV and human analysts alone. [260]

The processing of LFR is almost instantaneous, allowing alerts to be issued and individuals to be intercepted immediately where police are deployed among the crowd under surveillance.[261] The technology can allow authorities to build and maintain a comprehensive record of a person's movements throughout public spaces wherever the technology is deployed.

While there are current technical limitations with facial recognition algorithms, particularly relating to the number of biometric profiles that can be processed at any one time within the field of view,[262] these constraints will likely be removed as commercial vendors build and improve the technology. Such technical limitations should not be relied upon as human rights safeguards.

The impact on the right to privacy (as well as other rights) can also be significant, depending on how watchlists are formulated, authorised and used. If the watchlist is too broad in its design or operation, it could result in a chilling impact on movement and individual autonomy through public spaces.[263] Indeed, the use of facial recognition in some countries clearly amounts to a breach of many fundamental rights and freedoms, which is, in large part, because of the extensive list of individuals tracked using the technology, including the many who are tracked to monitor 'social harmony' rather than for law enforcement purposes.[264]

---

[260] See, for example, this report about the proliferation of FRT enabled cameras throughout Jerusalem and the West Bank: https://www.theguardian.com/technology/2023/nov/11/west-bank-palestinians-surveillance-cameras-hikvision

[261] National Physical Laboratory, 'Equitability Study 2023', (n 18) [1].

[262] Ibid [1].

[263] *Glukhin v Russia*, (n 10) [88].

[264] Human Rights Watch, 'China's Algorithms of Repression' (n 155).

Depending on camera quality, lighting and other technical requirements, FRT could be deployed as an overlay to existing CCTV camera systems across cities without the awareness of those whose biometrics would be processed.[265] Adverse impacts on privacy rights are also engaged in the creation of watchlists on which the technology relies. Such impacts could be heightened where images are scraped from the internet without the consent or knowledge of the individuals concerned.[266]

For many people who are subjected to this technology, the impact on Article 8 is significant because they will be unaware that their biometrics have been processed by police.[267] Unlike other forms of biometric processing (such as fingerprints or DNA profiles), LFR can process a person's biometric data from a distance with no physical indication or impacts to notify an affected person that such processing is occurring. This in turn can adversely impact the ability for the individual to seek judicial oversight and obtain effective remedies where such processing is unlawful or disproportionate.[268] As the ECtHR has explained, such an outcome could reduce Article 8 to a 'nullity':

> [W]here a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions … The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation.

[265] Natalia Menendez Gonzalez, 'Development or dystopia?', (n 245), 89.

[266] ibid 89.

[267] *Bridges v SWP* (EWCA), (n 13) [20].

[268] The right to an effective remedy is enshrined in Article 13 ECHR.

> A right of recourse … for persons potentially affected by secret surveillance is to be derived from Article 25, since otherwise Article 8 runs the risk of being nullified.[269]

Analysing Article 8 for the purposes of assessing proportionality of LFR should consequently reflect the spectrum of potential rights impacts, as opposed to accepting the narrow formulation of rights impacts claimed by MPS. The technology could easily be extended by the police in a manner that would have far greater impacts on the right to privacy of individuals who are identified and tracked across public spaces by LFR.

While the use of LFR by the MPS is currently designed in a way that does not result in large datasets being combined to deliver comprehensive surveillance of individuals, there is nothing in the governance or approach of the MPS to suggest that future developments would not result in this type of surveillance.

Police from across the MPS will 'nominate' individuals who should be added to the LFR watchlist before any proposed deployment occurs.[270] It is the responsibility of the AO to consider and approve the inclusion of individuals on the watchlist.[271] This decision is a key locus of human rights analysis: if the requisite threshold for adding a person to the watchlist is too low, then it will result in a broad list that risks disproportionate and unjustified impacts on human rights. Equally, the thresholds must be linked to the powers and legal basis on which police use this technology: if the threshold is not correctly formulated and utilised, then it can quickly result in individuals being added to a watchlist without underlying legal authority, resulting in an unlawful impact on the human rights of the individual.

Requiring police to only utilise a specific list of wanted people (i.e. the watchlist) that is created for each deployment of LFR is a control against what could otherwise be wide scale surveillance, particularly if the technology was connected in real time to police intelligence systems (such as drivers licences and passports), which in turn would allow

---

[269] *Klass and others v Germany* App no 24952/94 (ECHR 6 September 1978) [36], cited with approval in *Szabó and Vissy v Hungary* App no 37138/14 (ECHR 12 January 2016) [33].

[270] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[271] Metropolitan Police Service, 'LFR: Legal Mandate', (n 6).

police to surveil and track people. This is a development that should be strongly guarded against, particularly (as has already been noted) the human rights repercussions would be significant were such systems to be brought together in this way.[272] The thresholds in place to govern the watchlist compilation are consequently a significant aspect to assess whether the use of LFR amounts to a justified interference with Article 8.

The AO is directed to focus on serious crime and public safety when compiling the LFR watchlist, but is not precluded from including individuals who are wanted by police for minor offences (and even where police seek out individuals from a welfare perspective).[273] A more appropriate criterion for inclusion on the watchlist would be to require a minimum offence threshold of individuals who are wanted for questioning for serious crimes where they are suspects, or they are fugitives/escaped from custody. Such thresholds should be based on legislation that precisely defines the criteria upon which an individual may be included on the watchlist.

Instead, the MPS governance directs the AO to consider three broad categories relating to criminal offences being investigated or pursued in determining whether to add an individual to the watchlist:

a) The nature of the offending being targeted—in terms of (i) potential sentences for the crime types sought (ii) the use of violence and/or the level of coercion involved in the offending, and (iii) the involvement of weapons.
b) The importance of addressing the crime issue—this includes (i) the level of organisation seen in relation to the crime types targeted (ii) the impact the crime is having or could reasonably be expected to have on the community, and (iii) the threat posed to public safety.

[272] Amnesty International, 'Ban dangerous facial recognition technology that amplifies racist policing' (2021) <https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/> accessed 5 June 2023.

[273] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

c) Examples where the seriousness of certain offences has been recognised—particularly where there are identified public protection considerations—this may include (i) the Serious Crime Act 2015, (ii) Schedule 15 of the Criminal Justice Act 2003 and (iii) Schedules 3 and 5 of the Sexual Offences Act 2003.[274]

Each category appears to prompt the AO to consider the seriousness (or otherwise) of the offences committed by the wanted person and the impact that such offences have on public safety. This does not, however, require the AO to explicitly consider and weigh up the human rights of the individual proposed to be added to the watchlist. Instead, the AO is required to consider overlapping and substantively similar aspects of the crimes allegedly committed and the risk posed by the individual wanted by police. The absence of any balancing between achieving a legitimate aim and the human rights of the individual is a significant gap in the MPS governance framework. It is also important to note that the MPS governance does not set a 'floor' below which the impacts on human rights would never justify the addition of a person to the watchlist, for example, because the offence they were sought in relation to did not justify the impacts on Article 8 stemming from the use of the surveillance.[275]

The categories of offence types (and other categories for which individuals may be included on the watchlist) are also arguably too broad, allowing the AO a significant degree of latitude to include a person on the watchlist who may be of interest to the police. This includes individuals who are:

a) wanted by the courts, and/or
b) suspected of having committed, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence or where

[274] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[275] See e.g., *Glukhin v Russia*, (n 10) [73].

there are reasonable grounds to suspect an individual depicted to be committing an offence, and/or

c) subject to bail conditions, court orders or other restrictions that would be breached if they were at the location at the time of the deployment, and/or
d) missing persons deemed at increased risk, and/or
e) presenting a risk of harm to themselves or others; and/or
f) who are the victim of an offence, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or is otherwise a close associate of an individual and that individual themselves would fall within paragraphs (a)–(e).[276]

In addition to considering whether an individual ought to be included on the watchlist with reference to their specific circumstances, the AO is also directed to consider the appropriateness of the inclusion of an individual on the watchlist in light of a set of factors relating to the proposed LFR deployment. These factors require the AO to consider:

a) [the] severity of [the] offence in question; this will often be relevant to the level of urgency associated with locating and arresting an individual. Many individuals change their behaviour, including the places they reside and frequent when they know they are wanted for a serious offence;
b) Risk; the level of risk associated with an individual, whether that risk is to the public or themselves;
c) Deployment location; the specific characteristics of the Deployment location may increase the possibility or likelihood of an individual passing through. For example, areas around transport hubs have a lot of people transiting from

[276] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

> place to place and other areas of London have 'pull factors' that make it likely that people from across London may frequent that area.[277]

Each of these categories that shape the decisions of the AO in creating the watchlist are broadly formulated and not framed with reference to a proportionality assessment in light of the rights impacts that will result from the inclusion of an individual on the watchlist. The MPS governance also fails to establish any circumstances in which the inclusion of an individual on the watchlist would never be justified in light of the resultant human rights impacts from such an inclusion, such as the inclusion of political activists[278] or of individuals whose inclusion would result in the unlawful operation of the system.

The risk that a person poses 'to the public or themselves' is also too broad and permissive as a threshold factor to be proportionate.[279] Under these guidelines, the AO could justify the inclusion of individuals for a wide range of risks, extending from individuals wanted for allegedly committing murder (posing a risk to the community), right through to children who have left care homes without authorisation and who police seek to return to the care of the state (who may be at risk to themselves). While it may appear on paper that such a threshold is meaningful, in practice it is too broad and could be used to justify the inclusion of nearly any person of interest to police on a watchlist.

The ECtHR found the use of LFR by police to investigate minor 'administrative' offences amounted to unlawful interferences with Article 8.[280] Therefore, the discretion held by the MPS AO in determining whether an individual is included on a watchlist is arguably too wide in light of the legal thresholds that would otherwise apply to biometric processing by police.[281]

The MPS governance invokes 'lawfulness, proportionality and necessity' in directing the AO to undertake their responsibilities in assessing and approving proposed LFR

[277] ibid.

[278] See e.g., Undercover Policing Inquiry, < https://www.ucpi.org.uk/>.

[279] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[280] *Glukhin v Russia*, (n 10) [83].

[281] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

deployments but does not step through what this amounts to in assessing the lawfulness of including an individual on the watchlist. Is the AO expected to assess whether the biometric data held by the MPS is of sufficient quality to enable the LFR algorithm to accurately identify a wanted person who passes the zone of recognition? Is the AO expected to assess the intelligence held by MPS as to whether there is sufficient belief (or reasonable belief, or suspicion) the person will be in the vicinity of the camera when deployed?

It is also unclear what degree of analysis is expected from the AO in authorising a watchlist that contains the biometric profiles of many thousands of wanted people. The MPS governance appears to focus on the AO authorising broad categories that result in the ineffectual consideration of rights and provision of justifications for the use of LFR, rather than undertaking an analysis of the interferences with the rights of individuals impacted by their inclusion on the watchlist.

The MPS governance drafted to regulate the decisions of the AO in authorising the watchlist is consequently too broad, resulting in disproportionate impacts on Article 8.

The discretion exercised by police is broad, particularly when coupled with the lack of a requirement in the MPS governance for the AO to undertake a proportionality assessment considering the impacts on Article 8 and other human rights of the individual nominated to be included on the watchlist. This presents a real risk of arbitrary interference with the right to privacy and arguably results in disproportionate and unlawful interferences with Article 8.

The surveillance camera commissioner noted that LFR would be more likely to satisfy these requirements if it were 'deployed on a targeted or smaller scale basis and for a narrowly defined purpose.'[282] Reiterating and applying the Article 8 standards established in relevant jurisprudence, the commissioner noted the importance of police ensuring their deployment of LFR was 'targeted, intelligence led, time limited, and strictly necessary where other less intrusive options may be available.'[283] A key aspect of this is the intelligence on

[282] Office of the Biometrics and Surveillance Camera Commissioner, The use of overt surveillance camera systems in public places by police forces in England and Wales: An assessment of compliance with section 33(1) of the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice, (Report 2023), [15].
[283] ibid [15].

which police believe a person will be in the area where LFR cameras are deployed, which, as noted above, is not a basis on which the MPS governance is structured.

An additional element considered in the assessment of what is 'necessary in a democratic society' is the nature of the offences captured by the use of the technology.[284] In the *Glukhin* judgment, one factor leading to the ECtHR's conclusion of unlawfulness was that processing biometric personal data using facial recognition had been permitted 'in connection with the investigation and prosecution of any offence, irrespective of its nature and gravity'.[285] This resulted in a disproportionate impact on Mr Gulkhin's Article 8 rights, and consequently in a finding of a violation of Article 8.

The MPS adds individuals to the watchlist under a broad range of categories. The range is so wide that it is likely to fail both the legality and proportionality limbs of a legal analysis of Article 8(2). As previously noted, individuals who pose a significant risk to the broader community, or whose apprehension by police is for a similarly strong law enforcement purpose, could be proportionate to the rights impacts that result from LFR being used to locate them. But the open nature of the MPS's LFR analysis allows for the inclusion of lower-risk categories, which would more clearly result in a disproportionate impact on the Article 8 rights of affected persons.

To ascertain whether such Article 8 interference is proportionate, it is important to understand the use case or category of the wanted person under review. For some of the categories listed in the MPS governance, it is arguable that the interference is only useful or desirable, rather than necessary. This includes, for example, the inclusion of individuals wanted in connection with summary offences or investigations where they may be a witness. In both these examples, it may be desirable or expedient for police to include the biometrics of such individuals on the watchlist, but it is not justified in light of the disproportionate impacts on their Article 8 rights compared to the relatively marginal policing objectives expected from the use of LFR. In sum, it would likely be difficult for the State to establish that

[284] *Glukhin v Russia*, (n 10) [72]; P.N v Germany, (n 135) [72].

[285] *Glukhin v Russia*, (n 10) [87].

the aim was proportional to the means used to achieve them in respect of these watchlist categories.

The ECtHR would allow a margin of appreciation within which the state party can assess and pursue a pressing social need, where this results in interferences with Article 8.[286] While the margin of appreciation has permitted the retention of biometric information, including photographs, across different state parties to the ECHR (as summarised in Chapter 2), it is important to note the reference in the *Gaughran* decision to this potentially changing as technology presents further use cases for police that may increase the interference with Article 8.[287]

It is arguable that the ECtHR would draw on this concept to find that LFR uses that seek to identify individuals who pose a serious and imminent risk to community safety are necessary to achieve a legitimate aim, as the aim is proportional to the means used to reach it in light of the importance of achieving this public safety outcome. But the Court may not find that the lower-level categories of LFR use in the MPS governance would fall within the margin of appreciation, nor that such use cases amounted to a proportionate interference with Article 8.

When the AO compiles the LFR watchlist and approves the location, date and time of deployment, there is a requirement that they have formed the view that 'there are reasonable grounds to suspect' that a person on the watchlist will attend at a time or times when the LFR is deployed.[288] On paper this appears to be an entirely appropriate requirement made of the AO, but it is difficult to understand how this could work in reality, considering the size of the watchlist (with many watchlists exceeding 2,500 individuals) and the fact that, by definition, police will not know the precise location of any of the individuals on the watchlist at the time they identify them as being suitable for inclusion (if they did know their whereabouts, they would not need to resort to using LFR to find them). Therefore, it is unclear how the AO can be credibly satisfied that an individual person (multiplied by the

[286] *Big Brother Watch and Ors v UK*, (n 65) [361].

[287] *Gaughran v UK*, (n 9).

[288] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

thousands of individuals on the watchlist) is likely to be in the vicinity of any proposed LFR deployment. Police could have intelligence of sightings of individuals in a proposed area, but this threshold does not appear to accommodate the fact that such an analysis and authorisation must occur at the scale of the watchlist size.

Acknowledging this, the MPS directs the AO to consider the legality, proportionality and strict necessity of the inclusion of *offence types* for inclusion on a proposed watchlist rather than considering and authorising the inclusion of each individual person proposed to add to the watchlist.[289] The result is an ineffective oversight and an approval process that results in a large number of individuals being included on a watchlist simply because police want to apprehend them. This is not in line with human rights assessment to be undertaken by the AO, which should involve identifying the legal basis for processing a person's biometrics and including them on the watchlist. It should also involve balancing the police's operational objectives with the rights and interests of the person being surveilled, including those who are not on the watchlist but who will be affected by the technology.

AOs are directed to consider the necessity of deploying LFR to the proposed area, and whether the 'aims' of the deployment could be achieved in another location.[290] If the AO determines that it is necessary to deploy LFR in a particular area, they must consider the available mitigations when weighing the impacts on human rights that come from the deployment of LFR against the expected benefits.[291] The AO is directed to consider:

a) the reasonable expectations of privacy the general public may have at that location, with further guidance that 'some places by their nature attract greater privacy expectations than others' and the example of a busy inner city London thoroughfare compared with a quiet suburban park or backstreet; and further that LFR deployment should 'ensure the size and scale of the Deployment [will enable] those on a Watchlist to be effectively located without disproportionately processing excessive biometric data'

[289] ibid.

[290] Metropolitan Police Service, 'MPS LFR Policy Document', (n 7), [16].

[291] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8) [7].

b) if the proposed deployment attracts concerns by reference to those expected to be at the location ('hospitals, places of worship, legal offices, polling stations, schools and other placed particularly frequented by children, care homes and persons who may be attending a nearby assemblies or demonstrations') and whether individuals may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area, as a result of LFR deployment.[292]

On one level, this appropriately directs the decision maker (the AO) to think through the 'expectations of privacy' that the community will have in relation to certain spaces and to ensure any deployment does not 'disproportionately [process] excessive biometric data'.[293]

However, this governance does not draw any red lines to indicate where it would be unjustified and inappropriate to deploy LFR cameras. This could potentially allow police to deploy them in close proximity to all of the areas listed, where higher expectations of privacy exist, including areas of worship, legal offices and schools. As has already been noted above, the expectation of privacy is not the sole or determinative consideration in determining interference with Article 8.[294] The deployment of LFR cameras in such sensitive locations could result in significant human rights limitations for members of the public needing to access those places privately and in a manner that does not induce a fear of being identified by the police or the government.

As with other elements of the MPS's LFR deployment model, the parameters under which locations are determined leave a significant degree of discretion with the AO as the decision maker, without providing clarity as to how they must appropriately consider and balance the impacts on human rights against the operational objectives that may be achieved.

The breadth of categories under which a person may be added to the LFR watchlist by the MPS's AO (which, as outlined above, amounts to almost any person of interest to

[292] ibid [7].

[293] ibid [7].

[294] *Bridges v SWP* (EWHC), (n 21) [54].

police),[295] alongside the breadth of location types that the AO can authorise for deployment, results in a significant risk that rights interferences will be arbitrary and unjustified in any LFR deployment by the MPS.

The discretion exercised by police during LFR deployments also presents risks of arbitrary interferences with Article 8 and other protected rights of affected individuals. An example of this is the role played by police constables deployed to intercept and apprehend individuals who are identified by the system. Constables will exercise their existing police powers to ascertain the identity of the person and whether there are grounds for arrest or questioning, or whether the individual should be released. The MPS governance provides minimal information as to how this level of decision maker is expected to acquit their duties under human rights law in exercising their powers. This may be on the understanding that such governance is provided elsewhere to frontline police officers undertaking general duty policing tasks. However, this level of duty holder bears significant responsibilities to ensure any powers exercised are lawful, in pursuit of a legitimate aim, and necessary in a democratic society. Deployed police will use force to detain a person if required and will exercise arrest powers if they believe that the person in their custody is a wanted individual on the watchlist. Consequently, the MPS governance must address the protected human rights of individuals they apprehend and provide a greater degree of prescription in establishing the processes to be followed after the algorithm identifies a wanted person.

The MPS governance directs police to not impute guilt to a person who has been identified as a 'match' to the watchlist, but whose identity cannot be established or refuses to cooperate when pressed by police, and are further directed that such individuals are not automatically liable for arrest in these circumstances.[83] It is unclear whether an alert is a sufficient legal basis for an officer to form a 'reasonable suspicion' such that they can exercise their powers to apprehend and identify the individual. As with many other aspects of the MPS governance, police are instructed to use their judgment in assessing whether to

[295] Note this was one ground upon which SWP was found to have unlawfully deployed LFR: *Bridges v SWP* (EWCA), (n 13) [201].

engage with individuals who are uncooperative or who attempt to circumvent the system processing their facial biometrics:

> None of this means that [deployed police] cannot or should not engage with a member of the public as they would do in any other set of circumstances where someone's behaviour or presence gives rise to suspicion or the use of any other policing power where it is right and proper to do so.[296]

Consequently, it is left to police discretion as to whether a person who noticeably changes their path away from LFR is stopped, questioned and subjected to further checks of identity (such as fingerprint scanning). Police are directed to ensure any powers they exercise in such circumstances are justified and lawful.[297] Similarly, it is left to police discretion to respond to 'uncooperative' individuals who they stop following an alert being made by the algorithm.

Where the deployment model relies to some degree on the consent of individuals to have their biometric profiles processed by the system, it is notable that the discretion summarised here remains in the MPS governance. Police are directed that they should not impute guilt, but that they also have discretion to exercise their powers in apprehending the individual where their actions amount to an exercise of *not* consenting to have their sensitive biometric data processed by the algorithm.

Police are also instructed to consider not just the alert produced by the algorithm, but also the likelihood of 'subject, system or environmental factors' contributing either towards believing an individual is a true match to a person on the watchlist, or to discard the purported match made by the algorithm and not exercise any powers following an alert.[298] While this appears to provide some safeguards to govern decision making by police using LFR, it is important to also remember that this process may occur in a very short

[296] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[297] ibid.

[298] ibid.

period of time, from ten to twenty seconds after the initial alert is made (from when the individual walks through the 'zone of recognition' to when they have passed the police deployed in support of the operation.[299] There is no suggestion in the MPS governance that deployed police will have any briefings or familiarity with any (let alone all) of the more than 2,000 individuals on the watchlist. It is unclear how officers are expected to assess the accuracy (or otherwise) of any matches made vis-a-vis the 'subject, system or environmental' factors suggested.

Consequently, while the MPS governance appears to direct police to undertake a 'fulsome' assessment before detaining a person matched by the algorithm, it is unlikely that there will be sufficient time for such an assessment to occur before the individual in question has passed police and vanished into the crowd. This results in the risk that both the LFR operator and police officers deployed outside will be more likely to rely solely on the results produced by the algorithm in matching any person to the watchlist. There is a meaningful risk of confirmation bias resulting from the MPS deployment model.

Independent research undertaken in 2018 of MPS use of LFR, which included direct observance of a number of LFR deployments, noted the briefing processes for deployed police included instruction on how to weigh and assess recommendations from the algorithm of matches:

> All observed officer briefings were clear on the importance of human discretion in the LFR process. Officers were consistently instructed that a computer derived match was not sufficient to confirm an identity in and of itself. This is appropriate given the significant error rates associated with LFR and legal stipulations concerning meaningful human intervention in digital decision-making processes.[300]

This is a positive observation that would suggest officers were well equipped to understand and use LFR technology as a supplement to their own professional assessment of whether it

[299] ibid.

[300] Pete Fussey and Daragh Murray, *Independent Report on MPS use of LFR*, (n 26) [13].

is appropriate to apprehend an individual. However, the same research observed that this briefing process did not appear to amount to any instances where an officer overrode the initial match made by the algorithm. Instead:

> every instance in which this simultaneous approach was followed led to an attempt to engage a matched individual. This forms part of a wider and discernible 'presumption to intervene'.[301]

This presumption to intervene raises questions about how effective the 'human in the loop' model devised by the MPS really is, particularly when it results in officers apprehending and questioning all people for whom the algorithm has made a presumptive match. While on paper the human in the loop may address the risk of arbitrary interferences with Article 8, in practice this does not appear to be the case. This presents some risk when the algorithm is affected by bias—for example, when the algorithm misidentifies a person of colour or a woman due to the training datasets upon which the algorithm has been built.[302] The safeguard deployed is to purportedly rely on the judgment of officers in identifying and not acting upon inaccurate matches. As was recently found in the Casey Review of the MPS, the organisation is institutionally racist, misogynistic and homophobic.[303] Giving human decision makers mere seconds to assess the output of the algorithm, coupled with systemic issues like police prejudice suggests the MPS governance does not appropriately address the risks to arbitrary, disproportionate and unlawful interferences with Article 8.

[301] ibid [13].

[302] See analysis relating to NPL evaluation, and Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Proceedings of Machine Learning Research 81: 1-15.

[303] Baroness Casey of Blackstock DBE CB, 'An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service' (March 2023) [329].

Deployment Details			
27 August 2017		Environment	Free flowing – no control
28 August 2017		Total duration	12 hrs 00 min
Crowd throughput	8440 per hour (estimate)	Watchlist size	528
Outcomes			
Crowd		**Bluelist**	
# Recognition opportunities	101000(estimate)	# Recognition opportunities	59
# Alerted	96	# Correctly Alerted	42
# Engaged	6		
# ID confirmed	1		
# Action	0		

Table 7 Notting Hill Carnival 2017: Deployment details and LFR outcomes

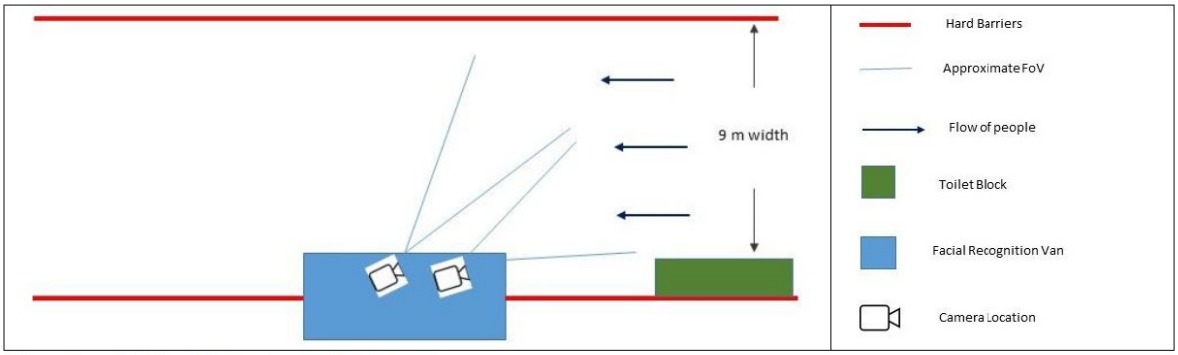


Figure 8 — Notting Hill Carnival 2017: Layout



Figure 9 — Notting Hill Carnival 2017: Example Footage

Diagram 5: LFR deployment Notting Hill Carnival, 27–28 August 2017[304]

Diagram 5 documents the deployment of LFR during the Notting Hill Carnival and is instructive in understanding the limitations of foreseeability in the deployment of LFR. The diagram notes the flow of people, with 8,440 people per hour moving through the area where the cameras were deployed, flowing between two 'hard barriers' past the zone of recognition. Over the deployed period appropriately 101,000 biometric profiles were

[304] National Physical Laboratory, 'MPS LFR Trials Evaluation 2016-2019', (n 40) [31].

processed. Deploying LFR in this way clearly maximises the opportunity for the technology to process large volumes of biometric data while minimising the opportunities for individuals to avoid having their biometric data processed by the tool. While signs (see Diagram 3) provide clear statements that individuals are not obliged to have their biometrics processed (i.e. they do not have to pass the sign and enter the zone of recognition), the cameras are deployed by design at 'pinch points' within which large crowds of people are corralled in a manner that maximises the opportunity for the cameras to scan their faces. This results in potential disproportionate impacts on rights. A large number of individuals have their biometric data processed, without a corresponding law enforcement 'benefit' (as seen in the low number of arrests made of wanted individuals, and a significant number of incorrect 'matches' being made by the algorithm).

The analysis above suggests that the MPS governance does not adequately address the requirement to demonstrate the interference with Article 8 is necessary in a democratic society. Police are not authorised to harness any technological advancement in aid of achieving their responsibilities, despite the human rights impacts that result from this adoption. The ECtHR has noted that contracting states are not lawfully permitted to adopt emerging technologies 'at any cost', as the use of such technologies in the criminal justice system without careful balancing between the benefits of the extensive use of these techniques against private life interests would result in 'unacceptably weakened' enjoyment of Article 8 protections by affected individuals.[305] While some of these use cases clearly do achieve the legitimate aim category while also remaining proportionate in light of their human rights impacts, others do not.

Less Restrictive Options

Police have powers to observe individuals in public places, which impacts Article 8 rights, but not to the extent that LFR use does. Although LFR deployment may be necessary and more effective than relying on human identification alone to identify individuals who pose a

[305] *S & Marper v UK*, (n 68) [112].

significant and imminent risk to the rights and freedoms of others, or to committing crimes, there are less restrictive options available than those deployed by the MPS. This includes locating individuals who are wanted for minor offences and do not pose comparable levels of risk to others in the community. Similarly, there are less restrictive alternatives for identifying vulnerable people, including victims of crime or potential witnesses to crime, that do not interfere as significantly with the privacy rights of those individuals (or the community at large) as the use of LFR does.

The MPS suggests that the use of LFR can minimise information sharing that may impact human rights and privacy. This is particularly important when LFR is used to locate missing persons or individuals with outstanding warrants. Media releases can have an indiscriminate impact and may negatively affect a person's reputation, especially when published online.[306] While this may be the case in theory, the current MPS operating model, whereby LFR is deployed in a specific geographical area for a specific time and purpose, could not replace the need for police to issue missing persons alerts in light of the number of people who go missing each year[307] and the size of London compared with the scale on which the technology can be currently deployed. However, this could change if the MPS deployed LFR at a larger scale, such as across London's public transport system, and on an ongoing basis.

The MPS appears to have provided examples in their governance documents where the use of LFR amounts to a less restrictive option on rights than the police response to an issue in the absence of using the technology. The example provided here may amount to comparatively less interferences, but it is unclear that it would be effective where LFR is deployed for a fixed period in a fixed and overt location.

In conclusion, there may be less restrictive options than LFR available to the MPS, but it depends on which use case the MPS seeks to address. In some circumstances the

[306] Metropolitan Police Service, 'Standard Operating Procedures for LFR', (n 8).

[307] Across MPS, there were 36,859 missing person reports between January and April 2021: Katharine Carpenter, 'How the Met Police deals with London's missing person reports' (14 July 2021) BBC, < https://www.bbc.co.uk/news/uk-england-london-57762720> accessed 5 February 2023.

risks posed by the wanted person to the community will justify the use of LFR. In other circumstances the adverse impacts on Article 8 will outweigh the operational objectives, particularly in light of the less restrictive options available to police to locate a person.

Conclusion

The MPS continues to deploy LFR surveillance despite community concerns, multiple evaluations highlighting biases and inaccuracies in how the algorithm operates, and the lack of a dedicated statutory foundation upon which the tool could be more clearly and lawfully used.

The publication of all MPS governance documents pertaining to LFR deployment allows for a deep dive into the model the police utilise for this surveillance. This analysis highlights the real risks of violations of Article 8 ECHR arising from the ongoing use of the technology. As the foregoing analysis has demonstrated, use of AI technology by the MPS, with a particular focus on LFR in this thesis, engages and interferes with Article 8 of the ECHR. This includes the rights of individuals whose sensitive biometric data are uploaded to the watchlist, the rights of individuals whose biometric data are processed by the deployed cameras and the rights of individuals apprehended by police when the algorithm makes a match between an individual at the deployment and the watchlist data.

The next question is therefore whether the interference is nonetheless justified by virtue of Article 8(2) ECHR. The analysis undertaken in this thesis demonstrates that it is not permissible in several respects. The lawful basis upon which the MPS relies to utilise LFR technology is partially sourced from the common law powers of the office of constable and partially from statutory powers including the PACE Act. Neither source of law is tailored to the contours and risks presented by this form of AI, with the result that the law utilised by the MPS remains broad, overly permissive of rights intrusions and ineffectual in protecting against arbitrary interferences with Article 8. The MPS governance, which is broad and ambiguous, does not establish any red-line protections for the core or essence of privacy protected by Article 8. It instead invokes legal and human rights terminology to justify decisions made by police to authorise and use the technology, but does not require decision makers to assess and ascertain whether their impacts on the human rights of affected people is lawful, pursues a legitimate aim, and is necessary in a democratic society.

The use of LFR by the MPS is arguably unlawful on this basis alone. However, considering the biases and limitations of the tool in relation to particular gender and racial groups, it can be argued that the MPS could face significant challenges in establishing that the use of LFR furthers a legitimate aim. If a person poses an imminent risk to community safety and LFR is unable to accurately identify them when they pass through the zone of recognition, the tool will have failed to assist police in apprehending the person, resulting in a decrease in community safety.

The safeguards the MPS has built into its LFR model are similarly ineffective. For example, deploying police officers to identify, understand and override biased outputs from the algorithm is clearly an ineffective failsafe. This is partially because the time available to the human in the loop is at most 10 to 20 seconds and also because the MPS culture has been identified as institutionally racist, misogynistic and homophobic.[308] Expecting this workforce, without further tailored training and support, to identify and address biased outputs in the tool is clearly ineffective and inappropriate.

Moreover, as demonstrated above, many of the uses of LFR do not meet the requirement of necessity in a democratic society as the aim is not proportional to the means used to achieve it. Less restrictive options to achieve the same policing aims are both present and commonly utilised by other police forces. The MPS's deployments of LFR have shown that while the tool can supplement police work to identify and locate wanted individuals, the algorithm has a low accuracy rate in identifying individuals from the watchlist. This may be due to the accuracy of the tool itself, but is more likely the fact that it requires a wanted individual to pass by the specific deployment location where the cameras are located, followed by a positive identification from the algorithm, for it to operate as planned.

While the MPS argues that the impact on rights—particularly for individuals who are not wanted and whose sensitive biometric data is almost immediately deleted—is minimal, this is arguably not the case. The use of this form of surveillance technology, alongside the

[308] Baroness Casey, 'Independent Review into MPS' (n 210) [17].

gradual push to make it more widely used, has a chilling impact on individual autonomy in public spaces and poses a real risk to the enjoyment of Article 8, and other, rights.

The MPS relies on the *Bridges* decisions to argue that their use of LFR technology is lawful. However, this thesis has shown that sufficient grounds exist to challenge the lawful interference of Article 8 where it is impacted by LFR. Ideally, the UK Parliament will enact tailored legislation to address the risks posed by this technology. If it does not, however, it will fall to human rights advocates to litigate for the protection of Article 8 rights and to stop the spread of this form of intrusive surveillance that presents significant risks to the enjoyment of human rights by millions of people across London.

Bibliography

Amnesty International, ‘Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing’ (*Amnesty International*, 2021) <https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/> accessed 5 June 2023

BBC Click, ‘Fines and Facial Recognition’ (YouTube, 2019) <https://youtu.be/0oJqJkfTdAg> accessed 1 February 2023

Big Brother Watch, ‘Face Off: The Lawless Growth of Facial Recognition in UK Policing’ (*Big Brother Watch*, May 2018), <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>

Brewster T, ‘London Police Facial Recognition “Fails 80% of the Time and Must Stop Now”’ *Forbes* (4 July 2019) <https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/?sh=75557c7ebf95> accessed 14 April 2023

Buolamwini J and Gebru T, ‘Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification’ (2018) 81 *Proceedings of Machine Learning Research* 1

Carpenter K, ‘How the Met Police Deals with London’s Missing Person Reports’ *BBC* (City, 14 July 2021) <www.bbc.co.uk/news/uk-england-london-57762720> accessed 5 February 2023

Casey L, *Baroness Casey Review: An Independent Review into the Standards of Behaviour and Internal Culture of the Metropolitan Police Service* (Final Report, March 2023)

De Cymru, H, South Wales Police, ‘Facial Recognition Technology’ (*South Wales Police*) <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/> accessed 1 August 2022

European Union Fundamental Rights Agency, *Preventing Unlawful Profiling Today and in the Future: A Guide* (Research Paper, Luxembourg, 2018)

Fussey P and Murray D, *Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology* (Human Rights Centre, University of Essex, July 2019)

Gentile G, *Does Big Brother Exist? Face Recognition Technology in the United Kingdom* (SSRN Research paper, 20 January 2023) <https://ssrn.com/abstract=4331633>

Gonzalez N M, ‘Development or Dystopia? An Introduction to the Accountability Challenges of Data Processing FRT’ (2021) 26 *Communications Law* 2

Human Rights Watch, ‘China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App’ (*Human Rights Watch*, 1 May 2019) <www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass> accessed 1 August 2022

Information Commissioner’s Office, *Information Commissioner’s Opinion: The Use of Live Facial Recognition Technology by Law Enforcement in Public Places*, (Official Paper, 31 October 2019, Reference 2019/01)

Johnson B, ‘Privacy No Longer a Social Norm, Says Facebook Founder’ *The Guardian* (London, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 11 April 2023

Land M K and Aronson J D, ‘The Promise and Perils of Human Rights Technology’ in Land and Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018)

Mansfield T, National Physical Laboratory, ‘Facial Recognition Technology in Law Enforcement Equitability Study: Final Report’ (NPL Report MS 4, 3 March 2023)

Mayor of London, ‘London Assembly, Questions to the Mayor: “Use of Fingerprint Scanners in the Met”’ (*London Assembly*, 16 July 2020), <www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/use-fingerprint-scanners-met-1> accessed 1 June 2023

Metropolitan Police Service, ‘About the Met: Jurisdiction’ (*Metropolitan Police Service*) <www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/jurisdiction/> accessed 1 August 2022

Metropolitan Police Service, ‘About the Met: The Met Has a Long and Rich History to be Proud Of’ (*Metropolitan Police Service*) <www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/met-museums-archives/important-dates/> accessed 1 August 2022

Metropolitan Police Service, ‘Advice and Information: Facial Recognition’ (*Metropolitan Police Service*) <www.met.police.uk/advice/advice-and-information/fr/facial-recognition> accessed 1 August 2022

Metropolitan Police Service, ‘Live Facial Recognition: Legal Mandate’ (Version 2.0) <www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-legal-mandate.pdf> accessed 15 June 2022

Metropolitan Police Service, ‘Live Facial Recognition: Process Summary’ (*Metropolitan Police Service*) <www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-process-summary-2023-web.pdf?__cf_chl_tk=9q.2Zcvy5w05xKt6dsxZwVdnSj_B4.ST.MDPBd4Jj98-1690250774-0-gaNycGzNDeU> accessed 11 April 2023

Metropolitan Police Service, ‘MPS LFR Policy Document: Direction for the MPS Deployment of Overt Live Facial Recognition Technology to Locate Person(s) on a Watchlist’ (Version 2.0)

Metropolitan Police Service, ‘Standard Operating Procedures for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology’ (Version 2.0) 7 <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf> accessed 15 June 2022.

National Physical Laboratory, ‘Metropolitan Police Service Live Facial Recognition Trials’ (Trial Period August 2016–February 2019, Published February 2020)

Ni Loideain N, ‘Lawfulness and Police Use of Facial Recognition in the UK: Article 8 ECHR and *Bridges v South Wales Police*’ (5 April 2023). Accepted for publication in R Matulionyte and M Zalnieriute (eds), *Facial Recognition in the Modern State* (Cambridge University Press, 2024)

Office of the Biometrics and Surveillance Camera Commissioner, *Commissioner for the Retention and Use of Biometric Material Annual Report January 2021–March 2022* and *Surveillance Camera Commissioner Annual Report March 2021–March 2022* (Report presented to Parliament pursuant to section 21(4)(b) and section 35(1)(b) of the Protection of Freedoms Act 2012; Published February 2023)

Office of the Biometrics and Surveillance Camera Commissioner, *The Use of Overt Surveillance Camera Systems in Public Places by Police Forces in England and Wales: An Assessment of Compliance with Section 33(1) of the Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice* (Report, 2023)

Purshouse J and Campbell L, ‘Automated Facial Recognition and Policing: a Bridge Too Far?’ (2022) 42 *Legal Studies* 209

Richards N, *Why Privacy Matters* (1st edn, OUP, 2021)

Ryder M, ‘Independent Legal Review of the Governance of Biometric Data in England and Wales’ (*Ada Lovelace Institute*, 2022) <www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf>

Science and Technology Committee, *The Work of the Biometric Commissioner and the Forensic Science Regulator* (HC 17, July 2019)

Topham G, ‘March of the Robots: How Biometric Tech Could Kill Off Paper Passports’ (*The Guardian*, 4 February 2023) <www.theguardian.com/politics/2023/feb/03/biometric-technology-paper-passports-redundant> accessed 11 May 2023

Undercover Policing Inquiry <www.ucpi.org.uk/> accessed 12 April 2023

Wachter S and Mittelstadt B, ‘A Right to Reasonable Inferences: Re-thinking Data Protection Law in an Age of Big Data and AI’ [2019] *Colum Bus L Review* 494