

## Government Response to the Justice and Home Affairs Committee's letter on Live Facial Recognition (LFR) technology

### Introduction

1. The government welcomes the opportunity to respond to the Committee's letter on the use of live facial recognition (LFR) technology by police forces in England and Wales.
2. We are committed to empowering the police to use the tools and technology they need, and the public expects them to use technologies like facial recognition (FR) to solve and prevent crimes, bring offenders to justice, and maintain public safety. We are working closely with industry and the National Police Chiefs' Council (NPCC) to keep pace with the rapid developments and improvements in LFR technology and to ensure that forces can use it in an effective, fair, and proportionate way. Far from perpetuating it as some still claim, FR has the potential to effectively eliminate bias in identification in the near future, as demonstrated by the independent testing by the National Physical Laboratory (NPL) of the algorithm South Wales Police (SWP) and the Met have been using.<sup>1</sup>
3. Your letter and other commentators have highlighted the fact that SWP lost the Court of Appeal case on LFR in *Bridges v SWP*.<sup>2</sup> That was a test case to clarify the law around police use of LFR, which the Court of Appeal did in its judgment, finding in favour of the appellant in three of the five grounds brought. However, since that judgment in 2020, the College of Policing (CoP) has issued national guidance in the form of an Authorised Professional Practice (APP) for LFR<sup>3</sup>, responding to the two areas of the law the judgment said needed to be clarified. These were the 'who' and 'where' questions as the judgment put it - i.e. what categories of people could be included in watchlists, and under what circumstances could the technology be used. The APP also includes a range of other safeguards such as the requirement that the police immediately delete the biometric data of anyone the system does not match to the watchlist. The judgment also found that SWP had not done enough to satisfy themselves about whether the FR algorithm they used does not have an inbuilt bias. As set out above, the NPL has since independently tested the algorithm SWP and the Met have been using and found them to be highly accurate with no statistically significant bias in terms of gender and ethnicity, at the settings they use.
4. LFR has helped the police to quickly and accurately identify people wanted for serious crimes and who pose a high risk of harm to others or themselves. An example of this was at the Arsenal v Tottenham North London derby in September last year, where the use of LFR led to three arrests. One person was charged with being in breach of a football banning order, one was wanted on recall to prison for sexual offences, and the final person admitted using threatening and abusive words and being in breach of a court order. More recently, it was deployed in Croydon and helped the Met identify and subsequently arrest individuals wanted for rape, grievous bodily harm, robbery and other serious offences. As well as disrupting and deterring crime, the use of LFR frees up police time and resources, allowing more officers to be out patrolling the streets, engaging with communities and carrying out complex investigations.
5. We recognise the importance of ensuring that LFR is used appropriately and there are safeguards in place to ensure this. Its use is governed by data protection, equality, and human rights laws, and can only be used for a policing purpose where necessary, proportionate, and fair. The CoP APP sets out when the police can deploy it, the categories of people they can look for, including the requirement to immediately delete the biometric data of anyone the system does not match to the watchlist of wanted individuals. Following a possible LFR alert, it is the police officer who decides first whether the alert is reasonable and then judges whether to engage with a person and only then what action, if any, to take after that.
6. All police forces routinely use retrospective facial recognition (RFR) to quickly identify suspects using the facial matching facility on the Police National Database (PND), which contains images of people taken on arrest. There are numerous examples where the technology has helped identify high harm offenders. For example, a man was jailed for life after attacking a woman he followed off a bus. He was arrested within 48 hours of the incident following the use of RFR on the images captured by CCTV. RFR was also used to quickly identify a man wanted for a knife attack on a bus driver in Tower Hamlets. He was charged with grievous bodily harm with intent and sentenced to more than 5 years in prison. In October last year, the Minister for Crime, Policing and Fire wrote to all Chief Constables and Police and Crime Commissioners (PCCs) encouraging them to double their RFR searches on PND. The PND algorithm has been updated to improve performance, and the NPL is testing it.
7. We understand the importance of transparency and providing information to facilitate public debate. We therefore published a facial recognition factsheet on 29 October 2023.<sup>4</sup> The Minister for Crime, Policing and Fire has also made regular public statements on police use of the technology, including in Parliament. The Met Police<sup>5</sup> and South Wales Police<sup>6</sup> have also published information on their use of LFR.
8. Looking ahead, we intend to publish a roadmap setting out the direction for FR over the next three years. This will include supporting forces to make greater use of LFR; enabling operator-initiated FR that would allow officers to verify the identity of a person of interest without having to arrest them or take them into custody; working with the NPCC to ensure consistency across policing in the retention, processing and use of custody images of people taken on arrest; and making it possible for the

<sup>1</sup> National Physical Laboratory independent testing - <https://science.police.uk/delivery/resources/operational-testing-of-facial-recognition-technology/>

<sup>2</sup> Bridges v South Wales Police Court of Appeal judgment - <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>

<sup>3</sup> College of Policing Authorised Professional Practice - <https://www.college.police.uk/app/live-facial-recognition>

<sup>4</sup> Home Office's police use of facial recognition factsheet - <https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/>

<sup>5</sup> Met Police's facial recognition page - <https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/>

<sup>6</sup> South Wales Police's facial recognition page - <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>

seamless searching of all image databases the police can access where necessary and proportionate, and subject to the proper governance and safeguards.

9. The Government's response to the Committee's recommendations is set out below. We are grateful to the Committee for reviewing this important subject and giving us the opportunity to respond.

## **Response to Recommendations/Request for further information**

### **A. Legal basis**

**Recommendation:** We note that, in contrast to the evidence we have received from the police, the Court of Appeal in the Bridges judgment expressed concerns about the “fundamental deficiencies” in the current legal framework arguing that “too much discretion is currently left to individual police officers” and that it is not “clear that there are any criteria for determining where AFR can be deployed” (see paragraphs 91 and 92 of the Court's decision). We are concerned that the findings of the Bridges case were specific to that case and that the case cannot be understood as a clear basis for the use of LFR. Whatever the practice, it requires a firm foundation in primary legislation.

#### **Government Response**

1. There is a comprehensive legal framework governing police use of LFR. This includes police common law powers to prevent and detect crime and bring offenders to justice, the Data Protection Act 2018 (DPA), Human Rights Act 1998 (HRA), Equality Act 2010 (EA), Police and Criminal Evidence Act 1984 (PACE), the CoP's APP on LFR, and published police policies.
2. A number of oversight bodies are active in this space including the Information Commissioner's Office (ICO), which regulates police use of LFR and has issued guidance, the Equality and Human Rights Commission (EHRC), and of course the courts. His Majesty's Inspectorate of Constabulary and Fire & Rescue Service (HMICFRS) also inspect, monitor and report on the efficiency and effectiveness of police forces.
3. The Court of Appeal did find that SWP's policies on who they were looking for and where LFR could be deployed gave them too much discretion. As described above, the CoP national guidance in the form of an APP addressed those shortcomings when it was published in March 2022.
4. The Court also confirmed that the detailed rules and policies do not need to be set out in legislation, and that SWP's own published policies constitute law for the purposes of “in accordance with the law”, as well as national guidance like the CoP APP.
5. While the case was brought against one police force, the judgment and the legal framework described above are applicable to all police forces in England and Wales that decide to use LFR.

**Recommendation:** We believe that there should be a legislative framework for the deployment of LFR technology. We invite the Government to explain in full how it has reached its own assessment, and whether it agrees with the Met Police's view that common law is sufficient for LFR deployment.

#### **Government Response**

6. As described above, there is a comprehensive legal framework for police use of LFR, which includes police common law powers. Specially on the common law, see paragraph 38 of the Court of Appeal judgment:

*“The Divisional Court held that **using cameras with AFR technology** to obtain the biometric data of members of the public in public falls within the common law powers of the police to obtain and store information for policing purposes, and that the **compilation of the watchlists** is both authorised under the Police and Criminal Evidence Act 1984 and within the powers of the police at common law. This is not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy AFR Locate [LFR]”.*

### **B. Framework for Deployment and Regulation**

**Request for further information:** We are concerned by the way that the use of the technology is being expanded to other police force areas by this process, which seems to leave discretion to the recipient police forces in how to employ LFR. Please explain in detail how this process operates, including the safeguards that apply, the contractual role of the software provider, and what liability rests with the providing force when the technology is used in these situations.

#### Government Response

7. SWP have previously provided their LFR equipment and expertise to Essex Police and Northamptonshire Police. This mutual aid process to support other forces to utilise LFR has the appropriate safeguards to ensure the recipient force meets the established legal and ethical standards, along with the standards set out in the CoP APP. In practice, this includes the recipient force establishing the appropriate in force governance and the completion of a robust suite of policy documents, prior to any deployment. The recipient force is the Senior Responsible Owner (SRO) and authorising officer and has the legal liability for any claims.
8. Mutual aid deployments to date have resulted in SWP providing the hardware (e.g. vans, server), software (FR algorithm) and resources (operators that deliver LFR), with their officers acting under the direction and control of the Chief Constable of the recipient force.
9. An SWP designate is present to support the use of LFR and consults with the recipient force's police command regarding the deployment. If at any point the designate has concerns that the deployment is no longer proportionate in meeting the objectives it was authorised to achieve, the deployment of LFR would stop and be escalated through to the recipient force's SRO, who is the decision maker in regard to the ongoing deployment of LFR. SWP is able to veto/decline a mutual aid request at any point where the strategic considerations in the host force exceed the tipping point for deployment.
10. This type of collaborative working between forces is not new and is what the public expect. It is important that forces share their knowledge and expertise to bring offenders to justice and keep the public safe. All forces using LFR have to comply with the comprehensive legal framework described above, including all the safeguards, whether using their own equipment or not.
11. As the police are operationally independent from government, we cannot provide any information on the contractual relationship between SWP and NEC.

**Recommendation: To ensure consistency, as LFR technology is rolled out, we recommend the adoption of a national compulsory training programme and standards for England and Wales to which all police forces must adhere.**

#### Government Response

12. The CoP APP sets out the importance of providing training to officers using LFR technology. This includes how to respond to an alert, the technical capabilities of LFR, the potential effects on those subject to any data processing, the principles of human rights, data protection and equalities legislation, how these are relevant to LFR, and the potential impact of the level of intrusion on data subjects.
13. Only 4 out of the 43 police forces in England & Wales have used LFR and a small number of officers within those forces. As its use increases, the NPCC and the CoP will consider the training and standards needed.

**Request for further information: How is “serious crime” defined and is the definition standard for all forces? How does any definition impact the police’s assessments of necessity and proportionality when deploying LFR technology in a particular situation.**

#### Government Response

14. LFR can only be used for a policing purpose and must be necessary, proportionate and fair. While the focus of LFR use is on tackling the most serious crimes and vulnerabilities, as described to you by the police representatives, it can be used at the same time to tackle less serious offences. Indeed, the Divisional Court said that by including all those who were wanted on warrant, there was potentially a considerable additional benefit to the public interest, without any impact on Mr Bridges.
15. The CoP APP sets out the categories of people that can be included on watchlists, which depends on the nature of the deployment. They include people who are wanted on warrants, suspects, missing persons, vulnerable people and people who could be a danger to themselves or others. In each case there needs to be appropriate justification and authorisation, always passing the tests of necessity, proportionality and use for a policing purpose.

**Request for further information: We are concerned by the fact that watchlists include people who “have an intent” or are thought to “threaten” to commit a crime. Such evaluation is most sensitive. What precisely does it mean? Should the approval of watchlists be carried out by a third independent party, outside the police force itself?**

#### Government Response

16. The CoP APP sets out the categories of people that can be on watchlists, which include individuals the police have reasonable grounds to suspect are about to commit an offence or present a risk of harm to themselves or others. Their inclusion on a watchlist must be approved by an officer of at least the rank of superintendent.

17. The use of LFR by Northamptonshire Police at Silverstone was part of a wider policing operation to help them identify offenders and keep the public safe given the risks associated with major sporting events. Their decision to use of LFR may have been in response to what happened at the same event the previous year.
18. The police have a common law duty to keep the public safe, this is a core part of their role and what they are trained to do, and so the government thinks that they are clearly the best placed to determine the composition of their watchlists, with the appropriate safeguards in the legal framework.

**Recommendation: We recommend the publication of national regulation or at the least guidelines, kept under review, on how extensive crowd-scanning activity is being assessed with relation to its lawfulness, necessity, and proportionality, before and after the deployment of LFR.**

#### Government Response

19. As described above, there is a comprehensive legal framework for police use of LFR and it includes numerous safeguards. The Court of Appeal in Bridges considered this legal framework and recognised that for those passing the LFR system, the right to a private and family life under Article 8 ECHR is engaged. However, when looking to the total numbers of people passing the LFR system, the court also decided that it 'is not a question of simple multiplication' and an 'impact which has very little weight cannot become weightier simply because other people are also affected'. The value of LFR to policing and the public cannot be assessed by simply comparing the total numbers of those passing the LFR system to the resulting arrests only, but needs to look wider to its ability to disrupt and deter criminality and keep the public safe. Accordingly, the Court of Appeal rejected Mr Bridges ground for appeal that the divisional court erred in finding that the use of LFR was proportionate.
20. The Court of Appeal did not find that the use of LFR needed to be limited to only serious offences. It decided that those sought by the police as being suspected of having committed criminal offences and those subject to a warrant issued by the courts are objective grounds for its use. The government respectfully rejects the claim that arrests made by the Met Police in 2022 did not relate to serious crimes. They included individuals wanted: in connection with an allegation of making threats to kill, for extradition on drug and violence offences, for the assault of an emergency worker and offences related to the possession and intent to supply class A drugs. There have been many more arrests since then, including for rapes, grievous bodily harm, and robbery.
21. The potential sentences crimes attract, the level of violence and/or coercion involved, offences involving weapons, and addressing the issue of crime, especially by reference to its impact on the local community and the risks to public safety are all important considerations. Some of the arrests made were related to court warrants issued for a wider spectrum of offences where a person has failed to attend court and a warrant has been issued for their arrest. Acting on court-issued warrants has a wider public interest in upholding the effectiveness of the criminal justice system.

**Recommendation: Given the importance of choosing who ends up on a watchlist, we recommend that watchlists should be subject to specific compulsory statutory criteria and standardised training.**

#### Government Response

22. As described above the CoP APP sets out the categories of people that can be included on watchlists, and the necessary authorisation required. It requires that watchlists are specific to a policing operation or for a defined policing objective. All officers using LFR receive training on its use. The APP also requires that forces have a standard operating procedure document setting out the decision-making steps for use of technology and the criteria for watchlists.

### **C. Public Confidence**

**Recommendation: Current means of letting the public know that LFR is to be, and is being, deployed are insufficient. Pre-deployment communication must be standardised through a national, clear and enforceable procedure.**

#### Government Response

23. As described above, there is a clear legal basis and framework governing police use of LFR, with oversight. The CoP APP covers the importance of providing the public with information about when LFR is used. Public information signs indicating its use are prominently displayed, and officers engage with the public to explain the technology and hand out leaflets with more information. Police forces also share information on their social media platforms. The relevant forces have also published key policy documents e.g. legal mandates, standard operating procedures and data from each deployment. This shows openness and transparency and is a good model for how forces should approach transparency and accountability.

**Recommendation: We agree that local engagement about the deployment of LFR is crucial in maintaining public trust about the technology. Public attitudes towards the use of LFR technology should be regularly assessed.**



#### Government Response

24. A number of polls conducted over the years, most recently in October 2023, have shown strong public support for police use of LFR. The government and policing recognise the importance of local engagement, especially with under-represented groups, in building and maintaining public trust and confidence. The CoP APP sets out the importance of proactive engagement with communities to build trust and confidence in the use of LFR and the need to explain how issues such as privacy, equality and transparency are addressed.

**Recommendation: Keeping the ‘human in the loop’ means that the ultimate decision about when to act following an alert must be that of a trained officer. To make sure that this applies in practice and that human/technology interaction is truly meaningful, we recommend that the Home Office requires feedback from LFR operators and reports publicly on this.**

#### Government Response

25. The CoP APP sets out the requirement for the human in the loop, which is an important safeguard in the comprehensive legal framework. LFR is an evolution of using police spotters to identify people of interest. Although algorithms have been shown to be increasingly accurate, they only suggest possible matches, not definite ones, and cannot engage with the public or arrest them – only police officers can do that. The government therefore does not see the need to ensure that this happens in practice. In any event, the Data Protection Act 2018 also covers the requirement for human decision making and is regulated by the independent ICO, who would be the appropriate body to consider this.

**Recommendation: Policing capabilities are largely amplified through the use of LFR technology. We recommend that information is required to be put in the public domain about the processes that are followed once a member of the public is approached by a police officer, including when they are told that they have been identified following the use of LFR technology.**

#### Government Response

26. Police officers have always been able to use their training and skills to spot a person who is wanted for a crime and then use their powers to stop them in the street. The difference with LFR is the ability in real time to scan a crowd against a watchlist, instantly eliminating the vast majority and highlighting a small number of people of potential interest for the police to consider approaching.

27. In October last year, the government published a facial recognition factsheet setting out how the technology is used, what happens following an alert, and the requirement for police forces to inform the public when they intend to use the technology, and where they can obtain more information on its use. As described above, the CoP APP sets out extensive guidance on the use of LFR and police forces have also published extensive documentation about how they use LFR.

**Recommendation: Greater consideration should be given to how explainability can be embedded in the LFR system.**

#### Government Response

28. It is important to ensure that algorithms are independently tested for accuracy and bias, which the NPL has done. They found that the algorithm the Met Police and SWP have been using to be highly accurate and fair at the settings they use. More specifically, for LFR they found that:

- There was a 90% chance of identifying someone on the watchlist, and at worst 1 in 6,000 false alerts. In practice since then the false alert rate has been far better than that. SWP have not generated any false alerts which is likely because their watchlists are much smaller than the Met's.
- There were no statistically significant differences in performance in terms of race or gender.

29. The CoP APP requires police forces to seek documented evidence from vendors as to how effective their algorithms are and the datasets they use.

### ***D. The Technology***

**Request for further information: We are concerned that crucial evaluations in LFR deployment are confined to split-second assessments, increasing the risk of human error.**

#### Government Response

30. As set out above, the LFR system only suggests possible matches, not definite ones. It is the police officer who decides first whether the alert is reasonable, and then judges whether to engage with a person and only then what action, if any, to take after that. Where the person is potentially wanted, as with normal investigations the officer must form reasonable grounds to suspect the person identified by the system is responsible for the commission of an offence, and that there is justification for an arrest. The standard procedures for investigations, evidence collection, arrest, charge, and prosecution must be followed.

**Recommendation:** As the human operation of the technology is essential to its success, we believe that there should be a national training programme and standard that all police forces can adhere to in their use of LFR. This would ensure that newcomers would have the advantage of learning from best practice.

Government Response

31. Training is the responsibility of the police and the College of Policing. As Ms Chiswick pointed out the NPCC is already considering this, which makes sense as the police interest in using LFR is increasing.

**Recommendation:** We recommend that regulations and standards include the introduction of appropriate institutional safeguards to ensure independent scrutiny of the technology.

Government Response

32. As set out above, it is important to ensure that the algorithm is independently tested, which the NPL has done. The CoP APP requires police forces to seek documented evidence from vendors as to how effective their algorithms are and the datasets they use.

## ***E. Regulation & Oversight***

**Recommendation:** The Committee recommended in 2022 that in order for the ATRS to become a “satisfactory register of algorithms in the public sector”, it should become mandatory, with entries being reviewed by a central body with the power to issue penalties if the ATRS was not completed. We reiterate that recommendation.

We question whether the ATRS has been sufficiently publicised to public sector bodies, such as police forces, by the Government. We repeat our 2022 recommendation that the completion of the ATRS should become mandatory.

Government Response

33. The Department for Science, Innovation and Technology (DSIT) is responsible for the Algorithmic Transparency Recording Standard (ATRS). The Central Digital and Data Office and the Centre for Data Ethics and Innovation (CDEI) developed the ATRS collaboratively with civil society groups and external experts. The ATRS was piloted with a variety of public sector bodies including police forces and the reports were published.<sup>7</sup> Following the pilots, the ATRS was updated to reflect feedback, and the CDEI plan to review it every 6 months.

34. The Home Office will work with DSIT and the Cabinet Office (as joint owners of the ATRS) to assess the best approach to implementing this requirement in policing, working closely with the NPCC lead for AI in policing. It is important to note that policing is operationally independent from government and held to account by elected Police and Crime Commissioners (PCCs). The NPCC recently endorsed a new ‘Covenant for Using Artificial Intelligence in Policing’ which sets out the principles forces should follow when using AI in the course of their business.

**Recommendation:** We question whether local, generalist ethics panels and committees are sufficient as ethical oversight for LFR deployment. A national ethics committee or board with subject expertise could improve this oversight and we recommend consultation with the police as to the establishment of such a committee.

Government Response

35. It is an operational matter for the police whether and how to use technologies like LFR to carry out their duty to protect the public. They are accountable to the PCCs or Mayors and they also take external advice as appropriate. The court has set out how the police can carry out LFR lawfully, and as set out above the CoP has implemented the judgment in its APP. The APP sets out a wide range of safeguards, building on the Bridges judgment. These include when LFR can be deployed, the categories of people they can look for, the requirement for deletion of the biometric data of anyone the system does not match to the watchlist, and the importance of public notification and engagement.

36. LFR has already demonstrated significant benefits in helping the police to tackle crime. The police have made multiple arrests of the most serious offenders, which include individuals wanted for rape, grievous bodily harm, robbery, possession of an offensive weapon and burglary.

37. As stated above, the algorithm the Met and SWP have been using has been independently tested by the NPL and was found to be highly accurate and fair at the settings they use.

38. Ethics panels have already reviewed police use of LFR, for example the London Policing Ethics Panel report from 2019, which the Met accepted in full.

---

<sup>7</sup> Algorithmic Transparency Recording Standard pilot reports - <https://www.gov.uk/government/collections/algorithmic-transparency-reports>

39. More generally the Biometrics and Forensics Ethics Group (BFEG) is an independent advisory body, which provides independent ethical advice to the Home Office and organisations within the Home Office remit including the police, on the collection, use and retention of biometric and forensic material, and on the use of large and complex datasets. BFEG took part in the public consultation on the CoP APP guidance.
40. BFEG is planning to run a pilot scheme to act as the national advisory body for ethics in digital and data matters for law enforcement. Working with the Association of Police and Crime Commissioners (APCC) and NPCC, their desired aim is to co-design the pilot to start in April this year. The pilot would focus on the provision of specific advice on the ethical considerations involved in the use of new technologies and matters within the remit of BFEG. In April 2025, following the completion of the pilot, an evaluation would then be conducted to review the suitability of installing BFEG as the national policing ethics advisory body.

**Recommendation: We do not consider the current methods of oversight sufficient. We recommend that scrutiny panels, as recommended for Stop and Search, should be employed for LFR also.**

Government Response

41. There is already substantial oversight of police use of LFR which, as set out above, is now an established and highly accurate technology as demonstrated by independent testing, with significant public safety benefits and safeguards.
42. The ICO as a regulator has enforcement powers which include issuing warnings, reprimands, enforcement notices and fines, and has investigated police and commercial use of LFR and issued guidance. The EHRC is also a regulator that can conduct investigations and issue legally binding agreements with organisations that break equality and human rights laws. HMICFRS inspect, monitor and report on the efficiency and effectiveness of police forces and publish their findings. The Independent Office of Police Conduct hold the police accountable for their actions to improve police practices. As the Bridges case demonstrates, the police are also subject to the courts system.

**Request for further information: We question why there is such disparity between the approach of the UK and other democratic states in the regulation of LFR.**

Government Response

43. Nearly 70% of police forces globally have access to some form of facial recognition technology (source: Comparitech 2021) and it is for each country to determine how they choose to regulate technologies like facial recognition. The UK is leading the way in the use of LFR in a clear and transparent way.
44. As set out above, the use of LFR has been tested by the courts and found lawful. The technology has demonstrated significant benefits in helping the police to tackle crime, and there are significant safeguards in place. When used, police must comply with data protection, equality & human rights laws, CoP APP and published police policies. Following a possible LFR alert, it is always a police officer who decides what action, if any, to take. Before a deployment, the police inform the public where they intend to use the technology and where they can obtain more information on its use. The NPL has tested the algorithm used by the Met and SWP and found it to be highly accurate and fair at the settings they use.
45. The government has a duty to keep the country safe by equipping the police with the powers and tools they need. This means supporting them in embracing technologies such as LFR and empowering them to use it safely, while maintaining public trust.

**Recommendation: Primary legislation could be kept up to date. We do not believe that regulation, which can more easily be kept up to date, has kept up with technological advances. Current regulation is additionally likely to be inadequate for future technological developments. Technological advances are so rapid that regulation needs to be kept up to date and agile, without constraining users. Several of our recommendations above point to the need for regulation.**

**We believe that, as well as a clear, and clearly understood, legal foundation, there should be a legislative framework, authorised by Parliament for the regulation of the deployment of LFR technology and make these recommendations accordingly.**

Government Response

46. As set out above there is already a comprehensive legal and oversight framework for police use of LFR, with significant safeguards. This includes primary legislation - the DPA 2018, HRA 1998, EA 2010 and PACE 1984. Those Acts are supplemented by the CoP APP and published force policies. The government thinks that principles-based primary legislation, supplemented by specific laws aligned to those principles, is the right approach to ensure that the legal framework can keep up with rapidly developing technology like LFR.

## **Annex: Material contained in the Government Response**

Annex A - College of Policing LFR APP

1. Guidance Overview
2. Live Facial Recognition
3. Watchlist
4. Where – date, time, duration and location of deployment
5. Key Performance Metrics
6. Terminology

Annex B - Facial Recognition Technology in Law Enforcement Equitability Study Final Report - March 2023

Annex C - Facial Recognition Deployment Processing Summary

Annex D - Facial Recognition Terminology Overview - Met Police

Annex E - Met Police - Live Facial Recognition – Data Protection Appropriate Policy Document

Annex F - Met Police Live Facial Recognition - Legal Mandate

Annex G - MPS LFR Policy Document

Annex H - Police use of Facial Recognition Factsheet Oct 2023

Annex I - R-Bridges-v-CC-South-Wales-ors-Judgment

Annex J - South Wales Police - Live Facial Recognition Legal Mandate

Annex K - South Wales Police - Policy Document for the Overt Deployment of Live Facial Recognition Technology

Annex L - South Wales Police - Standard Operating Procedure for the Overt Deployment of Live Facial Recognition Technology

Annex M - Standard Operating Procedure for the Overt Deployment of Live Facial Recognition Technology - Met Police

# Live facial recognition - Guidance overview

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist, in order to locate persons of interest by generating an alert when a possible match is found.

This module provides guidance for the overt deployment of live facial recognition (LFR) technology to locate persons on a watchlist.

## Tags

Digital intelligence and investigation

# Live facial recognition

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022

Written by College of Policing

17 mins read

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed (or multiple feeds) of faces against a predetermined watchlist, in order to locate persons of interest by generating an alert when a possible match is found.

This module provides guidance for the overt deployment of live facial recognition (LFR) technology to locate persons on a watchlist.

## Introduction

LFR is being used by forces for a number of policing purposes, including:

- supporting the location and arrest of people wanted for criminal offences
- preventing people who may cause harm from entering an area (for example, fixated threat individuals, persons subject to football banning orders)
- supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (for example, stalkers, terrorists, missing persons deemed at increased risk)

The technical operation of LFR comprises of the following six stages.

### 1. Compiling or using an existing database of images

The LFR system requires a watchlist of reference images, against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the facial features associated with their subjects are extracted and expressed as numerical values. This Authorised Professional Practice (APP) outlines considerations relevant to lawfully compiling a watchlist, including determining which persons may be on a watchlist and the sources of watchlist imagery.



## 2. Facial image acquisition

A camera takes digital pictures of facial images in real time, capturing images as a person moves through the zone of recognition and using it as a live feed. The siting of the cameras, and therefore the LFR deployment location, is important to the lawful use of LFR. This APP outlines considerations relevant to the locations where forces may select to deploy cameras when using them for LFR.

## 3. Face detection

Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

## 4. Feature extraction

Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template.

## 5. Face comparison

The LFR software compares the biometric template with those held on the watchlist.

## 6. Matching

When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the alerts and make a decision as to whether any further action is required. In this way, the LFR system works to assist police personnel to make identifications, rather than the identification process being conducted solely by an algorithm.

Chief officers will need to establish a suite of policy and operational documents, in line with this APP, that will detail the framework for operating LFR in their force and the standard operating procedures that will be employed.

A summary of the wider legal and ethical governance framework is shown at [Appendix A](#).

## Purpose and scope of LFR

This APP is consistent with the [‘Facing the camera’](#) guidance produced by the Surveillance Camera Commissioner (SCC) and the Surveillance Camera Code of Practice, issued pursuant to section 30(1)(a) of the Protection of Freedoms Act. Chief officers should continue to have regard to both documents.

The APP aims to:

- facilitate a national consistency of approach to the overt deployment of LFR technology to locate persons on a watchlist
- provide police forces with guidance on the overt use of LFR in a legally compliant and ethical manner, to enable forces to achieve legitimate policing aims
- provide members of the public with reassurance about the police use of LFR technology, and offer guidance to forces as to how the use of LFR should be foreseeable and accessible to everyone passing an LFR system
- establish the governance arrangements for the deployment of LFR

## Out of scope

There are other forms of facial recognition technology (FRT) that are not the subject of this guidance. These include retrospective facial recognition (RFR), also often referred to as ‘post-event’, which relates to non-real-time searching of images against a database. An emerging variant of FRT is near-real-time searching. This may be facilitated by way of a facial recognition app, where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR, in that a human operator has made the decision to submit a particular image for analysis, and is also out of scope for this guidance.

This APP relates to the overt use of LFR to locate those on a watchlist. It is important that forces who operate LFR and their decision makers are familiar with the [Regulation of Investigatory Powers Act 2000 \(RIPA\)](#). This is to ensure that they can identify any risk arising from their LFR deployment constituting covert surveillance, including when operating an overt camera system. Being aware of RIPA, and of when it applies, will reduce the risk of covert surveillance being conducted outside of the provisions of the relevant legislation. It will also ensure that the guidance of a RIPA authorising officer is sought in appropriate circumstances.

The appellant in the Bridges case raised the possibility that a large network of linked CCTV systems across the country could be connected to LFR and used to track a person's movements around the country. Use of LFR to track an individual in this way is out of scope for this APP, as this APP focuses on deployments of LFR where the focus is on locating a person passing a camera system, rather than seeking to track a person across a series of camera systems.

This APP focuses on the use of LFR by police forces. Out of scope is:

- any use of LFR systems operated by private companies and/or other public sector organisations
- instances where policing may share data to the operators of such LFR systems
- instances where policing may receive a CCTV feed from systems operated by private companies and/or other public sector organisations for the purposes of policing running LFR on the CCTV feed

The involvement of third parties beyond law enforcement, and the sharing of data to such third parties, raises additional data protection considerations beyond the scope of this APP. An opinion recently issued by the Information Commissioner on [the use of live facial recognition in public places](#) does provide guidance in this area.

In summary, this APP does not extend to:

- manually instigated facial recognition for retrospective searching of video or still images
- human-initiated, near-real-time facial search submitted from a mobile device (or similar)
- tracking a person's movements around the country across a number of systems
- any use of LFR systems outside of law enforcement operated by private companies and public organisations, or data sharing for the purpose of facilitating the use of those systems by forces
- any covert use of LFR

## Legal context

This APP gives direction to forces that will enable them to ensure that their deployment of overt LFR is in compliance with applicable legal requirements. It has been written taking into account legal judgments on LFR ([August 2020](#)). This APP also pays regard to the opinions, guidance and other documentation issued by the [SCC](#) (now the Biometrics and Surveillance Camera Commissioner) and the [Information Commissioner](#). This APP will continue to evolve to reflect changes in legislation, regulation, technology and accepted use, but is not a substitute for expert

legal advice, which forces should obtain to support their use of LFR.

## Legal framework

Chief officers with responsibility for deployment of LFR operations will need to satisfy themselves of the legal framework for its deployment in specific operational settings. Operational commanders will need to satisfy themselves that their proposed use of LFR complies with this APP, relevant legislation and force policies, based on their use case.

This APP gives direction on considerations relevant to the use of overt LFR to locate people on a watchlist. However, usage by forces will vary to reflect their specific use case for LFR, in line with their crime needs and policing priorities. As a result, chief officers should develop force policies to satisfy the legal points covered by this APP, with particular regard to the way in which operational use of LFR in their force area reflects:

## Further information

Where forces are processing for non-law enforcement purposes, when UK GDPR applies, requirements for processing special category (biometric) data will need to be taken into account.

- common law policing duties
- Police and Criminal Evidence Act 1984 Code D
- the Human Rights Act 1998
- the Data Protection Act (DPA) 2018
- UK General Data Protection Regulation (GDPR)
- the Protection of Freedoms Act 2012
- the Equality Act 2010

## Human rights considerations

Chief officers should be aware that LFR engages Article 8 in relation to persons passing the LFR system and persons being added to a LFR watchlist for location. LFR also has the potential to raise wider human rights considerations. These need to be considered by chief officers, with advice from force legal teams, in the context of their particular deployment plans and their policy for using LFR, but may include consideration of the following:

- Articles 2 (right to life) and 3 (prohibition of torture and inhuman or degrading treatment), in the context where an alert is generated by the LFR system and, if confirmed, the person located would pose a real and immediate threat to life. Similarly, this may arise for individuals sought in relation to offences where Article 3 is engaged. In this context, forces should be aware of the potential positive 'Osman' duties arising, and should therefore consider their capability and capacity to respond to such alerts in a timely fashion.
- Article 9 (freedom of thought, conscience and religion), in the context of where an LFR deployment is located, as well as the clothing that people wear. In normal circumstances (other than when a section 60AA Criminal Justice and Public Order Act 1994 order is in place), the police do not have a legal power to require persons to remove clothing simply because they are passing the LFR system. Officers should make use of the National Decision Model (NDM) when considering requests to remove articles of clothing.
- Articles 10 (freedom of expression) and 11 (freedom of assembly and association), especially if there are plans to use LFR in policing an assembly or demonstration where there may be a risk to the public safety from persons who need to be identified. This requires very careful consideration, supported by force legal advice, to ensure that LFR is a necessary and proportionate policing tactic to maintain public safety while minimising impact on those who wish to lawfully express their views or peacefully assemble with others.
- Article 14. This right requires that all of the rights and freedoms set out in the Human Rights Act 1998 must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and have equal access to them. The protection against discrimination is not 'freestanding'. To rely on this right, you must show that discrimination has affected your enjoyment of one or more rights in the act. However, you do not need to prove that this other human right has actually been breached. The use of LFR will be relevant in circumstances where demographic performance of the LFR algorithm varied to such an extent that people of a particular demographic were more or less likely to see a false alert generated against them. As a result, there are two points to consider in relation to the LFR system:
  - Does the LFR system's demographic differential performance vary by a particular demographic, such as it results in a person suffering a discriminatory effect?
  - If there is a difference in treatment, is there an objective and reasonable justification?

- Force policy documents (See force policy documentation): Force-level policy documents are also important in the lawful use of LFR. They should set out how the force will use LFR for legitimate policing purposes. These documents should be published unless doing so would compromise operational policing tactics. In relation to the overt use of LFR to locate persons on a watchlist, the publication of policy documents will help the public understand how a force, as a public body, will use LFR. This is an important safeguard for LFR to be used in a way that is in accordance with law, accessible and foreseeable to the public, and also helps retain the public trust and confidence in the police. Force policy documents should include detail setting out the criteria for developing a watchlist and possible sources for watchlists, as well as where the LFR system may be deployed and for what purpose.

## Public sector equality duty

The public sector equality duty (PSED) is relevant to forces when considering, using and reviewing any use of LFR. The PSED also formed an important ground of appeal in the [Bridges case](#), particularly in the context of forces taking reasonable steps to understand their LFR system's algorithm in relation to its statistical accuracy and demographic performance on an ongoing basis.

- Noting that the PSED is a non-delegable duty, chief officers need to be able to demonstrate their compliance with their PSED obligations arising from section 149 of the Equality Act 2010, which are as follows:

*A public authority must, in the exercise of its functions, have due regard to the need to:*

*- eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act*

*- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it*

*- foster good relations between persons who share a relevant protected characteristic and persons who do not share it*

Studies have suggested that there is potential for some facial recognition algorithms to be biased, in terms of their performance with respect to different demographic groups. However, not all algorithms behave in the same way. The 2019 National Institute of Standards and Technology

(NIST) report on [Demographic Effects in Facial Recognition Systems](#) concluded that the accuracy of LFR algorithms is improving year on year, and that the most accurate algorithms produce many fewer errors. It is therefore imperative that when considering procurement of LFR systems, an assessment of the general accuracy of the algorithm and its performance across different demographics is undertaken as part of PSED review.

Accuracy of facial recognition may be influenced by the data sets used to train its capabilities. It may not be possible to establish the exact nature and composition of vendor training data sets. However, forces should seek documented empirical evidence from vendors as to how effective their algorithm is, with respect to accuracy and performance across different demographic groups.

The responsibilities that arise from the PSED do not just apply to the LFR technology, the cameras and the software. They also apply to all aspects of the proposed conduct, including the role of the decision-making officer. The overall approach has to be considered and assessed as part of the PSED

Forces should address the PSED through the following.

- The completion and ongoing review of an equality impact assessment (or other similar recorded assessments of equalities considerations), to demonstrate that due regard has been given to the PSED.
- Satisfying themselves that everything reasonable that could be done has been done, to ensure that the software does not have an unacceptable bias on any basis, including on the grounds of race, sex, religion or belief. No system is ever 100% non-biased. There is always something within the system (and operator). Forces need to identify and understand the degree to which this occurs and then mitigate against this.
- Ensuring that there is rigorous oversight of the chosen algorithm's statistical accuracy and demographic performance – vendor claims must be tested to ensure that any procured algorithm is suitable for the force's use case and compliant with that force's PSED duties. The algorithm's performance should be reviewed if the force's use case changes.
- Ensuring that the force's use of LFR, the performance of its algorithm and any mitigations that the force uses to ensure its compliance with the PSED are subject to ongoing review, and that all reasonable steps continue to be taken to provide assurance of PSED compliance.

For further information see:



- Alvi M, Zisserman A and Nellåker C. (2018). 'Turning a blind eye: Explicit removal of biases and variation from deep neural network embeddings'
- Amini A, Soleimany AP, Schwarting W, Bhatia SN and Rus D. (2019). 'Uncovering and mitigating algorithmic bias through learned latent structure'
- Klare BF, Burge MJ, Klontz JC, Bruegge RWV and Jain AK. (2012). 'Face recognition performance: Role of demographic information'

## Force policy documentation

A chief officer should be designated senior responsible owner (SRO) with responsibility for overseeing the strategic management of LFR, addressing the issues below. The SRO should oversee the development of an overarching policy document that details their force's approach to using LFR, with a commitment to the following:

- Using overt LFR technology in a responsible, transparent, fair and ethical way, in accordance with all relevant law and only when other, less intrusive methods would not viably achieve the legitimate and lawful policing objectives.
- Strengthening and consistently developing the accuracy and functionality of LFR technology.
- Building public trust and confidence in the development, management and use of LFR by working to a force LFR communication strategy that promotes proactive engagement with the public about the use of LFR and explains how issues such as privacy, equality and transparency will be addressed.
- Ongoing community engagement, through force's existing channels, to promote the use of LFR and address concerns – the Centre for Data Ethics and Innovation (CDEI) document '[Addressing trust in public sector data sharing](#)' provides further guidance.
- Developing chief officer and PCC (or equivalent) strategic governance, with separation from operational decisions and decision makers where possible, to ensure sufficient independence and rigour when reviewing a force's use of LFR.
- Maintaining good operational governance through a command structure that incorporates operational and technical leads for the deployment of LFR. Ensuring clear decision making and accountability, specifying that the authorisation given by an authorising officer (AO) to deploy LFR in support of a policing operation should be made by an officer not below the rank of superintendent, and should be recorded in writing.

- Transparently identifying, managing, and mitigating reputational and organisational risk to the force continuously learning from deployments, identifying lessons to learn from each deployment.
- Maintaining the security of both the LFR system and data contained within it.
- Liaising with independent regulators where appropriate.
- Identifying the metrics against which the success of deployments will be judged, including setting the force's targeted false alert rate in policy and continuously assessing the success of deployments against these metrics, to ensure ongoing proportionality of its use and to provide reassurance regarding the ongoing performance of the technology and algorithms.
- Ensuring that when LFR is used to locate those on a watchlist and there is no match with a person on the watchlist on passing the LFR system, the biometric template created by the facial recognition technology should be instantaneously (or near instantaneously) and automatically deleted, without need for any human intervention. False positive alerts should be deleted as soon as possible and in any event within 31 days. This will facilitate the public's right to exercise their individual access rights and aligns with CCTV retention periods.

In cases of urgency, force policy documents may provide that an officer below the rank of superintendent, but not below the rank of inspector, may authorise the deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency. All authorisations should comply with the requirements set out below.

Situations where there is a need for an authorisation to be granted urgently include:

- an imminent threat to life or of serious harm to people or property
- an intelligence or investigative opportunity with limited time to act, the seriousness (in terms of threat, harm and/or risk) and benefit of which supports the urgency of action

If an authorisation is given under the urgency criteria above, the information and rationale should be recorded. Force policy documents should make clear that it shall be the duty of the AO who gives authorisation to inform an officer of the rank of superintendent or above, as soon as practicable, that LFR has been deployed and the reasons why. It is then for the superintendent (or above) to authorise the deployment to continue, making changes to the authority as they deem necessary, or to direct that it should stop.

If a further law enforcement purpose is identified after the AO has issued their authority for an LFR deployment, the AO should revise their authorisation. Such revision would consider the lawfulness,

strict necessity and proportionality of using LFR to meet the further law enforcement purpose, as well as its compatibility with the original law enforcement purpose.

## Supporting policy documentation

Chief officers should oversee the development of a number of other documents to supplement this APP. These include the following.

- LFR Authorisation Process Guidance Flowchart, or an equivalent document, which clearly sets out the decision-making steps to use LFR.
- LFR Standard Operating Procedure, or an equivalent document, which should include details of:
  - factors to consider relating to the force's use case and policing priorities for LFR
  - criteria for watchlists and sources of imagery
  - guidance when an alert is generated, actions to be taken following an alert, the resourcing of deployments to respond to alerts, and relevant officer policing powers
  - factors to consider when deciding on deployment location and camera placement
  - arrangements to ensure that the deployment is overt, including considerations regarding any prior notification and signage
  - responsibilities of officers and staff involved in deployment
  - retention periods
- Data protection impact assessment (DPIA), as required by section 64 of the DPA 2018, which addresses the types of deployment authorised by chief officers. Advice on the surveillance camera element of the DPIA can be found on the [SCC website](#).
- Equality impact assessment (EIA) or equivalent, which enables the force to demonstrate its compliance with the PSED for the types of deployment that the force intends to undertake.
- Community impact assessment (CIA).
- LFR training materials ensuring that those within the force who use LFR technology fully understand:
  - how to respond to an alert
  - the technical capabilities of LFR
  - the potential effects on those subject to any processing of biometric data
  - the core principles of human rights, data protection and equalities legislation, and how these are relevant to LFR

- the potential impact of the level of intrusion on the data subject
- An appropriate policy document covering sensitive processing of data, pursuant to the DPA 2018 and relating to LFR. Section 35 (5)(c) of the DPA 2018 requires that, at the time the processing is carried out, the controller (chief constable) must have an appropriate policy document in place. The ICO provides forces with guidance and a [template](#) for this document, and the document should be made available to the ICO on request. Section 42 of the DPA 2018 specifies what this document is to contain, including:
  - an explanation of how the processing complies with the relevant data protection principles
  - an explanation of the controller's policies in relation to retention and erasure, including an indication of how long the data is likely to be retained

The schematic at [Appendix B](#) details the steps to be taken when planning an LFR deployment.

## Command structure

Force policy documents should also outline a command structure for the operational deployment of LFR, which should ensure separation between force-level strategic oversight for LFR and other roles. This should include individuals with responsibility for force-level strategic oversight for LFR, for authorising a specific LFR deployment (the AO), and for LFR deployment 'on the ground' (an operational commander), ensuring separation between these three roles. The below structure is one way to achieve this, although the structure and the terminology used may differ in order to meet the policing need for each force.

Gold – in strategic command of force LFR deployments, the force SRO.

Silver – the AO for the operation, responsible for the actions in sections 8.

Bronze – the operational commander 'on the ground' overseeing the operation in real time.

## Operational governance, oversight and command structure

### Criteria for deployment

Each deployment should be appropriately documented, assessed and authorised. Where an AO is not immediately able to provide their decision in relation to an application to use LFR in writing, their authorisation may be given verbally. Verbal authorisation should then be recorded in writing by the AO as soon as is practicable and, unless urgent, prior to the deployment of LFR.

The nature of the deployment should be informed by the force's policing requirements and their use case for LFR, with all deployments being:

- targeted
- intelligence-led
- time-bound and geographically limited when set within the context of the relevant use case

## Force operational documentation

Prior to the overt deployment of LFR in public spaces to locate persons on a watchlist, the AO should ensure that a number of documents, or equivalents, are completed. The documents should be supported by the assessments outlined in table 1.

Based on these assessments, a decision will be made as to whether an LFR application should be submitted to the AO. On consideration of the application and the assessment documents, the AO will then decide on whether to complete a written authority document.

Taken together, the LFR application and written authority document should do the following.

- Outline and approve the legitimate aim of the deployment, as authorised by the AO, and the legal powers that are being relied upon to support the deployment. It should explain how individual rights have been balanced against the benefits of using LFR.
- From a Human Rights Act 1998 perspective, articulate:
  - how and why the deployment is necessary (not just desirable)
  - Why it is proportionate to achieve the legitimate aim of the deployment
- From a Data Protection Act 2018 perspective, articulate how the processing of personal data is strictly necessary for law enforcement purposes, including:
  - what the 'pressing social needs'
  - why sensitive processing is needed to achieve the legitimate aim

- which of the schedule 8 grounds are satisfied
- why the purpose cannot be achieved through less intrusive means

The following documentation should support each LFR deployment.

**Table 1: LFR deployment documents and records**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assessments</b> | <p>These include a CIA, an EIA (or other similar documented record), a DPIA and the SCC’s self-assessment.</p> <p>These documents need to be considered by the AO when making an authorisation to ensure that they are sufficient to address the issues arising from the proposed deployment. The AO should involve their data protection officer in writing the DPIA and in managing the processing of personal data.</p> <p>The AO should ensure that issues have been adequately identified, documented and mitigated, to ensure that the deployment is both necessary and proportionate to the policing purpose.</p> <p>Documents such as the DPIA and EIA may be applicable across a number of deployments and, while they will need ongoing review to ensure sufficiency, they may not need revising for each deployment.</p> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Operational risk assessment**

A documented assessment of specific operational risks associated with an LFR deployment, including decisions taken regarding mitigation.

**LFR application**

The application explains how the proposed use of LFR is based on an intelligence case. The application should set out the details of a proposed deployment, including:

- location
- dates and times
- legitimate aim
- legal basis
- necessity
- proportionality
- safeguards
- watchlist composition
- resources

The AO should agree the date, time, location and duration of the deployment in advance, based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the policing purpose and intelligence case that supports the deployment. The deployment location will be determined by there being reasonable grounds to suspect that the proposed deployment location is one at which one or more persons on the watchlist will attend at a time, or times, at which they are to be sought by means of LFR. Those reasons should be recorded in a way that can be understood by an objective third person.



**Performance metrics**

A document detailing those metrics that will be gathered and used to assess the benefits of the operation. This may also be covered by forces in their LFR applications and/or in a force's LFR policy.

### Written authority document

The AO's written authorisation provides a decision-making audit trail demonstrating how the AO has considered the LFR application and is satisfied with:

- the accountability, legality, strict necessity and proportionality of the deployment
- the safeguards that apply to the deployment
- the alternatives were considered insufficient to realise the policing purpose

The document will detail (or, if covered in the LFR application and/or at a force policy level, authorise) the approach to:

- consistently clear and appropriate signage that takes full account of predictable routes
- how fair processing information will be made available in public spaces where LFR is being deployed and on police websites
- how individuals can exercise their rights under data protection law
- the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR deployment

The written approval should be retained in accordance with Information Management APP and other relevant legislation or policy, and should be made available for independent inspection and review as required.

|                         |                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LFR cancellation report | <p>Records details of:</p> <ul style="list-style-type: none"> <li>• where and when a deployment was carried out</li> <li>• the circumstances that brought a deployment to a conclusion</li> <li>• what resources were used</li> <li>• relevant statistic</li> <li>• outcomes</li> <li>• a summary of any issues following a post-deployment review</li> </ul> |
| Deployment logs         | <p>Logs completed in the planning and execution of an LFR deployment. For example, logs completed by the silver and bronze commanders, and by LFR operators.</p>                                                                                                                                                                                              |
| Register deployments    | <p>Forces should keep a register of all LFR deployments, which should be published.</p>                                                                                                                                                                                                                                                                       |

## Appendix A

Legal framework and governance.

## Appendix B

LFR summary process.

## Tags

Digital intelligence and investigation

# Watchlist

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022

Written by College of Policing

9 mins read

## Outline

This section covers the composition, generation and management of watchlists to be used in LFR deployments. The criteria for constructs of watchlists for use with LFR should be approved by the AO, and should be specific to an operation or to a defined policing objective. Watchlists, and any images for inclusion on a watchlist, should also be limited to the categories of image articulated in force policy documents, such as those set out below.

Force policy documents should also provide that the composition of watchlists:

- is based on the intelligence case
- is reviewed before each deployment, to ensure that all images meet the necessity and proportionality criteria for inclusion
- is not excessive for the purpose of the LFR deployment
- must only contain images lawfully held by police, with consideration also being given as to:
  - the legal basis under which the image has been acquired
  - the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk – the source of the image should be recorded
- should only use images where all reasonable steps have been taken to ensure that the image:
  - is of a person intended for inclusion on a given watchlist
  - is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the watchlist – regard should be paid to the prospect of the LFR system generating an alert if an older image is proposed for inclusion, where the person's facial features may have changed or aged significantly since the image was taken

- should be imported into the LFR system immediately prior to deployment and no more than 24 hours prior to the commencement of the deployment, to ensure that the watchlist is current – where the deployment is to last in excess of 24 hours, force policy should require an ongoing review of the watchlist, covering the issues of review, retention and deletion

## Specific considerations relating to protected characteristics

In December 2020, following the Bridges case, the then-SCC published a best-practice guidance document, '[Facing the camera](#)'. The SCC advocated the need to ensure that suitable controls exist around the placing of persons with protected characteristics on a watchlist. Any controls, mitigations and processes identified by forces will need to reflect their LFR system's performance and their particular LFR use case in order to satisfy their PSED obligations.

Force policy documents should identify any specific controls, mitigations and processes in response to points relating to demographic differential performance. Regardless of performance considerations, they should also recognise the need to take particular care when considering age, including the protection of children, particularly very young people and people with disabilities, for the following reasons.

## Further information

In relation to children, see [Detection and custody APP](#).

Their treatment in detention is governed not only by domestic legislation, but also by the [UN Convention on the Rights of the Child \(UNCRC\)](#).

- There may be different privacy expectations around the use of LFR that are particularly relevant in relation to these people, given their potential vulnerability.
- Forces will be aware that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic. If this is widely reported, people with that protected characteristic might be exploited by criminals to lower the risk of LFR detection. In this regard, forces should assess the risk to ascertain whether these persons are particularly susceptible to exploitation and coercion, and should take

steps to mitigate any risk arising.

In all cases, force policy documents should require that those undertaking each deployment should specifically identify and document whether the watchlist contains persons who are believed or suspected to:

- be aged under 18 years old
- be aged under 13 years old
- have a disability

A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) where such a disability may have an impact on the performance of the police force's LFR system. Examples that may have an impact (depending on the performance characteristics of the specific LFR system) include if the subject has had a facial injury, has undergone facial surgery, has a degree of facial trauma or is of a particular bearing that inhibits their facial features from being recognised.

In relation to safeguards to address greater expectations of privacy and given the potential for system factors relating to age, force policy documents should ensure that the use of age-appropriate privacy information is covered. They should also reflect that it is especially important to use a risk-based approach when locating individuals aged under 18 years old, with a particular focus on ensuring that the necessity case is fully made out.

## Further information

Studies have shown that young children up to the age of 13 are both harder to correctly recognise (lower true positive identification rate) but also harder to distinguish between (higher false positive identification rates).

The higher false positive identification rate may lead to more false alerts being generated against young children if there is an image of a young person in the watchlist.

If LFR will be used to locate a person and that person's records state that they are (or are suspected to be) aged under 13 years old, then system factors should be considered, including the ability for the LFR system to generate an accurate alert against the image proposed for inclusion on the watchlist.

If LFR will be used to locate a person and that person's records state that they have (or are suspected to have) a relevant disability, then there is a particular need to ensure that the image is suitable for inclusion on the watchlist. System and subject factors should also be considered, as well as the ability for the LFR system to generate an accurate alert against the image proposed for inclusion on the watchlist.

In both instances, prior to seeking authorisation from an AO, specific advice should be sought from force legal departments and from those advising on the technical performance of the LFR system. Where authorisation is then sought, this advice should be provided to the AO to help inform the decision-making process, and to allow them to record their decision regarding any inclusion on the watchlist and outline further safeguards that should apply.

## **Police-originated images that may be included on a watchlist**

Images that may be deemed appropriate for inclusion within an LFR watchlist include custody images of individuals and/or other police-originated images of people who are:

- wanted by the courts
- suspected of having committed an offence, or where there are reasonable grounds to suspect that the individual depicted is about to commit an offence, or where there are reasonable grounds to suspect an individual depicted to be committing an offence (see below)
- subject to bail conditions, court order or other restriction that would be breached if they were at the location at the time of the deployment
- missing persons deemed at increased risk of harm (see below)
- presenting a risk of harm to themselves or others (see below)
- a victim of an offence or a person who the police have reasonable grounds to suspect would have information of importance and relevance to progress an investigation, or who is otherwise a close associate of an individual and that individual would fall within people wanted by the courts and presenting a risk of harm to themselves or others (see below)

Where police-originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include:

- the purpose for which the police hold such images
- any processing limitations attached to the images
- the importance of including such images on a watchlist in order to meet a policing objective
- the proportionality of using such images on an LFR

## Non-police-originated sources of watchlist imagery

### Further information

Non-police images are images that were not taken under the direction or control of the police. They include images that may be provided by and/or sourced from public bodies, law enforcement partners (including those outside the UK), private companies and/or individuals.

Where it is viable to do so without unduly affecting the performance of the LFR system, force policy documents should provide that suitable police-originated images should be preferred for inclusion on a watchlist. However, there will be occasions where no image is held by the force or, if one is held, where its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police-originated image.

Non-police-originated should only be included in a watchlist with the authorisation of the AO. The AO should also consider all the circumstances pertaining to the image, in particular the factors stated above. The types of non-police-originated images that may be deemed appropriate for inclusion within an LFR watchlist are of people stated in the categories above.

## Interpretation of watchlist categories

### Missing persons deemed increased risk

This term will be subject to the College of Policing definition of medium risk (or above) that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.



## Presenting a risk of harm

This term will be informed by the intelligence case. This will need to inform the AO as to how:

- the individual presents a risk of harm
- using LFR to facilitate their location is necessary to manage the risk of harm identified
- why it is necessary for the police to take action in order to manage the risk of harm

The addition to the watchlist will also need to be a proportionate response to the need to manage the risk of harm. Addressing the risk of harm in this context will need to have a legal basis under a policing common law power or statutory power. 'Harm' may include a risk of harm arising in relation to a person's welfare and/or a financial harm, including as a result of fraud or other dishonesty. Harm can also arise if a person potentially poses a risk to national security.

Victim of an offence or a person who the police have reasonable grounds to suspect would have information of importance and relevance to progress an investigation, or who is otherwise a close associate of an individual, and that individual would fall within the categories mentioned in section 3 that may be deemed appropriate for inclusion within an LFR watchlist.

The necessity and proportionality threshold for any watchlist inclusion is high and the use of the category will be by exception. This is because, unlike the other categories, the person(s) sought are not at risk of harm and are not suspected of committing criminal offences. The necessity for inclusion should be based on a specific intelligence case, with the need for the inclusion on a watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to be able to demonstrate, to the AO's satisfaction, why the inclusion of a person in this category is necessary for one or more of the following:

- to help locate a person who is wanted by the courts and/or the police
- to advance the policing investigation
- to ensure their safety and/or the safety of others

The applicant would also have to demonstrate the proportionality of any inclusion on a watchlist. This would include considering the following.

- The rational connection between the inclusion of the watchlist and the objective.

- Any other less intrusive methods, as well as whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the watchlist is not made.
- The importance of locating the person sought, with reference to the threat, harm and risk that the addition to the watchlist addresses, balanced against the rights of the individual.
- Expectations of privacy, not least as victims and witnesses may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves. For any inclusion on the watchlist, the information they are believed to have should therefore be assessed to be of significant value to the police, or their location should be otherwise critical to ensure their safety and/or the safety of others.
- The measures to be taken to ensure the status of those included within this category is recognised by those involved in the operational deployment to ensure that the appropriate action is taken if an alert is generated. This might include the partitioning of the watchlist to distinguish between the different categories of subjects.

The then-SCC recognised the need for policing to locate victims, witnesses and close associates via LFR in his November 2020 guidance, '[Facing the camera](#)'. In this light, to assist forces and the wider public understand and foresee how this category may be used, the following are illustrative examples of where the need to add a person to a watchlist under this category may be made out.

| Status | Example circumstances                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Victim | Intelligence supports an assessment that a victim of crime is under a continuing clear threat to their welfare. Other less intrusive efforts to locate them have failed or are unviable in the time available and there is a need to locate them for their own safety. |

| Status                                            | Example circumstances                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Person reasonably suspected of having information | <p>The angle of the only CCTV from a violent gang-related knife attack does not show the faces of the perpetrators who remain at large. The footage does, however, show the faces of others who are reasonably considered to have seen the attack and it is clear that they should have had a good line of sight of it.</p> <p>If those people who are considered to have seen the offence can be located and they are assessed by the force as having relevant information that could be vital to progress the investigation, their location could help bring violent offenders who present a risk to society to justice.</p> |
| Close associate                                   | <p>A force has received information that a person wanted for a serious sexual assault has been receiving phone calls from a close associate. The associate is using public phone boxes to remain in contact and support the alleged perpetrator while they hide from the police. The associate is assessed as having relevant information that could be vital to progress the investigation. Other less intrusive methods have been used to locate the associate without success.</p>                                                                                                                                          |

## Tags

Digital intelligence and investigation

# Where – date, time, duration and location of deployment

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022 Updated 27 July 2023

Written by College of Policing

3 mins read

## Measures during an LFR deployment

Force policy documents should provide that signs (or other equivalent awareness-raising measures) that publicise the use of the technology should be used to inform individuals in advance of their entering the zone of recognition. This measure is to alert members of the public to the presence of LFR technology and to allow them sufficient time to exercise their right not to walk into the zone of recognition.

Forces should, unless in cases of critical threat when there is insufficient time, notify the public in advance of the deployment without undermining the objectives of the deployment. Details of the LFR are to be notified to the public using force websites and other appropriate communication channels (including social media).

Any member of the public who is engaged as part of an LFR deployment following an alert should, in the normal course of events, also be offered information about the technology. Any person who requires further information relating to LFR should be provided with contact information for the LFR operation.

## Privacy considerations relevant to an LFR deployment location

When reviewing a potential deployment location, AOs should also consider those who are likely to pass the LFR system, as well as the following.

- The reasonable expectations of privacy that the general public may have as a whole at that location:
  - some places attract greater privacy expectations than others
  - the number of cameras used actively by the LFR system should also be considered in this context, to ensure that the size and scale of the deployment enables those on a watchlist to be effectively located without unnecessarily processing biometric data
- Whether a proposed deployment location attracts particular concerns, by reference to those expected to be at a particular location. Where it is practicable to identify a member of the community as being responsible for a proposed deployment location (for example, outside a place of worship). Where that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate. Examples where those who attend may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area include:
  - hospitals
  - places of worship
  - centres for legal advice
  - polling stations
  - schools (and other places particularly frequented by children)
  - care homes
  - assemblies or demonstrations

If a deployment is necessary at a site that is focused on children or a protected characteristic, appropriate signage and information about the LFR deployment should typically be reasonably accessible to children or those with the protected characteristic who may pass through the zone of recognition. When assessing whether a deployment can be considered proportionate or not, consideration is needed as to the nature of the deployment and data processing that is proposed, as well as the effectiveness of the mitigations.

Where privacy or other human rights considerations are identified in relation to a particular deployment, the AO needs to consider the necessity to deploy LFR to that particular location and also consider whether the aims being pursued could be similarly achieved elsewhere. In instances

where that location is necessary (and the processing of data at that site is strictly necessary), AOs need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR system against the likely benefits of using LFR. This is to ensure that the policing action proposed is not disproportionate to the aim being pursued.

## Oversight bodies and regulatory frameworks

Chief officers should establish their own internal governance arrangements for LFR. This should involve chief officer and PCC (or equivalent) oversight, with separation from operational decisions and decision makers where possible, to ensure sufficient independence and rigour when reviewing a force's use of LFR. Forces should engage with local force ethics committees, or other suitable advisory structures, to help determine relevant oversight arrangements.

When considering the ethical deployment of LFR, chief officers should adopt an ethical framework within which they will operate. A national data ethics framework is under development.

It is important for the elected police body to be appropriately engaged and consulted with those decisions, which are within their statutory remit to make, particularly (but not exclusively) those associated with procurement, public engagement, performance and accountability.

The National Police Chiefs' Council (NPCC) Facial Recognition Technology Board oversees national policy in relation to LFR. The Board reports to the Joint National Biometric Strategic Board, which in turn reports to the NPCC National Crime Coordination Committee.

Forces considering deployment of LFR technology in the first instance should engage with the NPCC Facial Recognition Technology Board, who can offer appropriate support, guidance and signposting to other NPCC portfolios as appropriate.

## Other regulatory bodies

### Biometrics and Surveillance Camera Commissioner (BSCC)

The role of the [BSCC](#) is to encourage compliance with the Surveillance Camera Code, review how the code is working, and provide advice on the Code, including changes to it or breaches of it. Any force LFR system will need to comply with this Code and the 12 guiding principles. The guidance in this document applies those principles.

## Information Commissioner's Office (ICO)

The [ICO](#) upholds information rights in the public interest, as set out in data protection law. The DPIA must comply with sections 35-40 (principles 1-6) and section 64 of the DPA 2018.

## His Majesty's Inspectorate of Constabulary and Fire & Rescue Service (HMICFRS)

HMICRFS inspect, monitor and report on the efficiency and effectiveness of the police, with the aim of encouraging improvement.

## Tags

Digital intelligence and investigation

# Key performance metrics

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022

Written by College of Policing

2 mins read

This section outlines the minimum requirements and additional metrics or indicators that are relevant and suitable for collation and analysis for operational deployments. Additionally, as part of the force procurement process, due diligence should be given to expected algorithm performance (or accuracy).

The National Institute of Standards and Technology (NIST) regularly undertake large-scale facial recognition system tests. Although these provide a good starting point, it is incumbent upon the system owner to understand how these tests relate to the accuracy and equitability of their deployed algorithm. While publicly available test data from NIST can inform owners, it will usually be informative to measure accuracy of the specific operational algorithm on operationally realistic data.

There are two key metrics that determine the 'accuracy' of an LFR system and a third that details the time taken to generate an alert.

## True recognition rate (TRR)

This is also referred to as the true positive identification rate.

The TRR is the number of times when individuals on a watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times these individuals passed through the zone of recognition (regardless of whether an alert is generated).

This metric can only be generated by 'seeding' known subjects (for example, police officers or staff) into a [Blue Watchlist](#) and measuring the number of times those subjects are present in the zone of recognition against the number of alerts generated. Users of LFR systems (and vendors) should not focus so closely on maximising this metric, as it may increase the false alert rate to an extent that is



not possible to manage the number of false alerts.

## False alert rate (FAR)

This is also referred to as false positive identification rate.

This is the number of individuals who are not on the watchlist but generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition.

## Further information

The NPCC Facial Recognition Board are available to support decision making.

All of the TRR and FAR metrics should be recorded and reported to the SRO. Operational experience to date suggests that the FAR should be 0.1% or less (less than 1 in 1,000) in most scenarios. It should be noted that the number of false alerts generated is greatly affected by the number of subjects processed by the LFR system and, to a lesser extent, the size of the watchlist.

The configurable threshold (the point at which two images being compared will result in an alert) will have a direct impact on the TRR and FAR. The threshold needs to be set with care so as to maximise the probability of returning true alerts, while keeping the number of false alerts to acceptable levels, as determined by the SRO in light of the force's use case.

## Recognition time (RT)

This is the average time taken between a subject on the watchlist passing before a camera and the generation of an alert. Note that the actual amount of time taken to act on an alert will always be longer than the RT, as additional time is needed for the LFR operator to assess the alert and to pass it to an LFR engagement officer, who will then make a final decision on whether to engage or not.

The RT should be sufficiently small that an effective response to an alert is possible before the subject has moved too far from the point where the initial alert occurred. High-resolution video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

# Tags

Digital intelligence and investigation

# Terminology

This page is from APP, the official source of professional practice for policing.

First published 22 March 2022

Written by College of Policing

5 mins read

This section of the APP reflects terminology approved and adopted by the NPCC to facilitate forces working together in relation to LFR. It does this by promoting the consistent use of terminology and definitions, resulting in a commonality of language used by law enforcement agencies in England and Wales.

It is written to provide an accessible reference point for members of the public to understand the nature of LFR deployments, and for police officers seeking to use LFR operationally.

There are a number of technical terms that can be found within International Organization for Standardization (ISO) standards. It may be more appropriate to use these terms where a precise technical meaning is needed, for example, in relation to procurement.

## Terminology

### Adjudication

A human assessment of an alert generated by the LFR application by an LFR engagement officer (supported, as needed, by the LFR operator) to decide whether to engage further with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject factors, system factors and environmental factors

### Administrator

A specially trained person who has access rights to the LFR application, in order to optimise and maintain its operational capability.

### Alert

A notification generated by the LFR application when a facial image from the video stream, which is being compared against the watchlist, returns a comparison (similarity) score above the threshold.

## **True alert**

When it is determined that the probe image (the image from the video stream) is the same as the candidate image in the watchlist.

## **Confirmed true alert**

When, following engagement, it is determined that the engaged individual is the same as the person in the candidate image in the watchlist.

## **True recognition rate (TRR)**

The number of times when individuals on a watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times that these individuals passed through the zone of recognition (regardless of whether an alert is generated).

This is also referred to as the true positive identification rate.

## **False alert**

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement.

The false alert rate is one of the two measures relevant to determining application accuracy.

## **Confirmed false alert**

Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

## **False alert rate (FAR)**

The number of individuals who are not on the watchlist but generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition.

This is also referred to as false positive identification rate.

## Application accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the true recognition rate and the false alert rate. This is further explained below. The example given has been simplified to demonstrate the concept. Note that the metrics have been calculated in accordance with the agreed scientific method, as set out by the International Organisation for Standardisation.

The TRR, or true positive identification rate, would be 90% if, after 10 people on the watchlist pass the LFR system, a correct alert is generated for 9 out of 10 of those people. As no alert was generated against one person in this example, there was one missed alert.

The FAR, or false positive identification rate, would be 0.1% if, for every 1,000 people that passed the LFR system, an alert was generated against one person who was not on the watchlist.

## Authorising officer (AO)

The officer (usually holding the rank of superintendent or above) who provides the authority for LFR to be deployed.

## Biometric template

A digital representation of the features of the face that have been extracted from the facial image.

It is these templates (and not the images themselves) that are used for searching and that constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

## Blue Watchlist

A watchlist comprising of known persons that can be used to test system performance. For example, to measure the TRR, police officers and staff may be placed on a Blue Watchlist and 'seeded' into the crowd who walk through the zone of recognition during a deployment.

## Candidate image

An image of a person from the watchlist returned as a result of an alert.

## Deployment

The use of an LFR application, as authorised by an AO, to locate those on an LFR watchlist.

## Deployment record

An amalgam of the LFR application, the written authority document and the LFR cancellation report. This sets out the details of a deployment, including, but not limited to:

- location
- dates and times
- deployment and watchlist rationale
- legal basis
- necessity
- proportionality
- safeguards
- watchlist composition
- authorising officer
- resources
- relevant statistics
- outcomes
- summary of any issues

## Environmental factors

An external element that affects LFR application performance, such as dim lighting, glare, rain or mist.

## Faces per frame

A configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.

## Facial recognition

This technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database to generate possible matches. This is based on digital images (either still or from live camera feeds).

## False negative (missed alert)

Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are a number of reasons that false negatives occur, including application, subject and environmental factors, and how high the threshold is set.

## LFR engagement officer

An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering their questions and helping them to understand of the purpose and nature of the LFR deployment.

## LFR operator

An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

## Person(s) of interest

A person on a watchlist.

## Probe image

A facial image that is searched against a watchlist.

## Retrospective facial recognition (RFR)

A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.

## Subject factor

A factor linked to the individual, such as:

- demographic factors (for example, sex or ethnicity)
- wearing a heard covering
- smoking
- eating
- looking down at the time of passing the camera

## System factor

A factor relating to the LFR application such as the algorithm.

## Threshold

The configurable point at which two images being compared will result in an alert. The threshold needs to be set with care to maximise the probability of returning true alerts while keeping the false alert rate to an acceptable level.

## Urgency

In the context of authorising an LFR deployment, a deployment that is related to an:

- imminent threat-to-life or serious harm situation
- intelligence or investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action

## Watchlist

A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (reference image database) and will have been created specifically for the LFR deployment.



## Zone of recognition

A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.

## Tags

Digital intelligence and investigation

**NPL REPORT MS 43**

**FACIAL RECOGNITION TECHNOLOGY IN LAW ENFORCEMENT  
EQUITABILITY STUDY  
FINAL REPORT**

**DR TONY MANSFIELD**

**MARCH 2023**



Facial Recognition Technology in Law Enforcement  
Equitability Study  
Final Report

Dr Tony Mansfield  
Data Science Department

© NPL Management Limited, 2023

ISSN 1754-2960

National Physical Laboratory  
Hampton Road, Teddington, Middlesex, TW11 0LW

Extracts from this report may be reproduced provided the source is acknowledged  
and the extract is not taken out of context.

Approved on behalf of NPLML by  
Kevin Lees, Group Leader SED/DS/DATAAM

## CONTENTS

|           |                                                                                |           |
|-----------|--------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>SUMMARY .....</b>                                                           | <b>1</b>  |
| 1.1       | About the evaluation .....                                                     | 1         |
| 1.2       | Key findings – Retrospective Facial Recognition.....                           | 2         |
| 1.3       | Key findings – Operator Initiated Facial Recognition .....                     | 3         |
| 1.4       | Key findings – Live Facial Recognition.....                                    | 3         |
| <b>2</b>  | <b>EVALUATION OBJECTIVES .....</b>                                             | <b>5</b>  |
| <b>3</b>  | <b>DEMOGRAPHICS .....</b>                                                      | <b>6</b>  |
| 3.1       | Demographic categories .....                                                   | 6         |
| <b>4</b>  | <b>ASSESSING EQUITABILITY .....</b>                                            | <b>7</b>  |
| 4.1       | Statistical significance .....                                                 | 8         |
| <b>5</b>  | <b>OUTLINE OF METHODOLOGY AND DATA.....</b>                                    | <b>8</b>  |
| 5.1       | Cohort data subjects .....                                                     | 9         |
| 5.2       | Facial images of cohort.....                                                   | 10        |
| 5.3       | Video from Live Facial Recognition deployments.....                            | 11        |
| 5.4       | Filler facial images .....                                                     | 12        |
| <b>6</b>  | <b>EVALUATION RESULTS – RETROSPECTIVE FACIAL RECOGNITION.....</b>              | <b>12</b> |
| 6.1       | Methodology .....                                                              | 12        |
| 6.2       | Accuracy.....                                                                  | 13        |
| 6.3       | Low scoring mated comparisons & high-scoring non-mated comparisons .....       | 13        |
| 6.4       | Identical twins .....                                                          | 14        |
| <b>7</b>  | <b>EVALUATION RESULTS – OPERATOR INITIATED FACIAL RECOGNITION .....</b>        | <b>14</b> |
| 7.1       | Methodology .....                                                              | 14        |
| 7.2       | Accuracy.....                                                                  | 14        |
| 7.3       | Low scoring mated comparisons & high-scoring non-mated comparisons .....       | 15        |
| <b>8</b>  | <b>EVALUATION RESULTS – LIVE FACIAL RECOGNITION .....</b>                      | <b>15</b> |
| 8.1       | Methodology .....                                                              | 15        |
| 8.2       | Accuracy.....                                                                  | 18        |
| 8.3       | Demographic variations in False Positive Identification Rate .....             | 19        |
| 8.4       | Demographic variation in True Positive Identification Rate.....                | 20        |
| <b>9</b>  | <b>DISCUSSION .....</b>                                                        | <b>21</b> |
| 9.1       | Are demographic performance variations similar for LFR, RFR and OIFR? .....    | 21        |
| 9.2       | TPIR Variation in performance & equitability .....                             | 22        |
| 9.3       | FPIR Equitability .....                                                        | 22        |
| 9.4       | Effect of reference dataset/watchlist size and composition on FPIR.....        | 22        |
| 9.5       | Retrospective Facial Recognition performance on challenging facial images..... | 23        |
| 9.6       | Recognition against same-day image .....                                       | 24        |
| 9.7       | Suggestions for further investigations .....                                   | 24        |
| 9.8       | Test corpus arising from the study .....                                       | 24        |
| <b>10</b> | <b>TERMINOLOGY AND ABBREVIATIONS .....</b>                                     | <b>25</b> |
|           | <b>BIBLIOGRAPHY .....</b>                                                      | <b>27</b> |
|           | <b>ACKNOWLEDGEMENTS.....</b>                                                   | <b>27</b> |



# 1 SUMMARY

## 1.1 ABOUT THE EVALUATION

In August 2021 the Metropolitan Police Service (MPS) was awarded Home Office Science Technology Analysis & Research funding to undertake testing of the accuracy and equitability of Facial Recognition in an operational environment for three policing use cases:

- Live Facial Recognition (LFR)
- Retrospective Facial Recognition (RFR)
- Operator Initiated Facial Recognition (OIFR)

The National Physical Laboratory (NPL) was invited to submit a proposal and plan to conduct such an evaluation for MPS and South Wales Police (SWP), and a contract was awarded at the end of 2021.

The NPL test strategy [1] for an evaluation conformant with the standards ISO/IEC 19795-1 [2] and ISO/IEC 19795-2 [3] for biometric testing and reporting was agreed in April 2022. Noteworthy aspects addressed in the evaluation include:

**1:N identification:** The operational use cases evaluated use facial recognition for 1:N identification (rather than 1:1 verification).

**Face in video:** Live Facial Recognition involves identification of faces in live video.

**Real time processing:** Live Facial Recognition must operate in real time; the recognition decision must be given within seconds of the subject being videoed. To achieve this when there are many people in the field of view to be recognised, the algorithms may need to limit the number of faces processed per video frame or limit the number of video frames being processed.

**Operational environment and settings:** The evaluation uses face image and video data collected in the operational environment under operational settings.

**Accuracy, demographic variation & equitability:** The evaluation measures the accuracy of facial recognition, the variations in accuracy between different demographics, and assesses equitability, i.e., whether outcomes are broadly equivalent across demographics under operational use case settings.

**Under 18's:** The age range of the policing applications extends to those below age 18, and it is important to know whether performance is different for this demographic.

**Large demographically balanced datasets:** The testing of low error rates in a statistically significant manner requires large datasets. To achieve the required scale, the evaluation uses a supplementary reference image dataset of 178,000 face images (Filler dataset). This is an order of magnitude larger than the typical watchlist size of an operational Live Facial Recognition deployment. To avoid introducing a demographic bias due to reference dataset composition, a demographically balanced reference dataset was used, with equal numbers in each demographic category. For assessment of equitability under operational settings, the results from the large dataset are appropriately scaled to the size and composition of watchlist or reference image database of the operational deployment.



Data collection for the evaluation took place in July and August 2022 alongside five MPS and SWP operational deployments of Live Facial Recognition in London and Cardiff. A set of facial photographs were taken of a Cohort of subjects in a variety of settings. These Cohort subjects were seeded into the crowd flow to appear in the LFR video. Cohort subjects were not included on the operational deployment watchlists: an imperative to avoid interrupting the policing operation (and to reflect the safeguards of the data protection impact assessments regarding accurate data processing). Instead, the operational LFR video footage featuring the Cohort was saved to be re-played offline against the evaluation's Cohort and Filler watchlists at a later date.

The facial recognition technology and version tested is **NEC Neoface V4**<sup>1</sup> using **HD5 Face Detector**. These facial detection and recognition algorithms are those currently used by MPS and SWP for Live Facial Recognition, Retrospective Facial Recognition and Operator Initiated Facial Recognition.

The offline running of the data using the Neoface system emulating operational use, and our analyses of performance have taken place from September to November 2022.

This report sets out the findings of our evaluation, and is organised as follows:

- In the remainder of this section, we highlight some of the key findings of the study.
- Section 2 summarises the objectives of the evaluation.
- Section 3 provides details of the demographics assessed in the evaluation.
- Section 4 elaborates on criteria for equitability, and statistical significance of performance differences.
- Section 5 outlines the methodology, the image and video data collected for the evaluation and how it was used.
- Section 6 gives evaluation results for Retrospective Facial Recognition.
- Section 7 gives evaluation results for Operator Initiated Facial Recognition.
- Section 8 gives evaluation results for Live Facial Recognition.
- Section 9 provides further discussion on some of the findings and notes aspects that may be worthy of further testing or analysis.
- Section 10 provides a glossary of terms and abbreviations.

## 1.2 KEY FINDINGS – RETROSPECTIVE FACIAL RECOGNITION

Retrospective Facial Recognition is a post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them. For each identification search the system returns a candidate list of the records in the reference image database that best match the submitted probe image. The top  $R$  matches are returned for a pre-specified value  $R$ .

Recognition accuracy for Retrospective Facial Recognition is measured in terms of:

- True-Positive Identification Rate:  $\text{TPIR}(N, R, 0)$  - the proportion of 'mated' identification searches (i.e., where the subject has a record in the reference image database) that include the mated reference among the candidates returned.

TPIR depends on the number of candidates to be returned ( $R$ ), the number of records in the reference image database ( $N$ ). No face-match threshold is used in RFR.

---

<sup>1</sup> <https://www.necsws.com/facial-recognition-software>

### 1.2.1 In the evaluation, RFR always returned the correct reference identifier at Rank 1

For every probe image submitted for RFR in the evaluation, the correct reference identifier was returned at Rank 1 (i.e., as the top match). This is the best performance possible.

$$\text{TPIR}_{\text{RFR } 178400, 1, 0} = 100 \%.$$

It follows that TPIR is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable.

## 1.3 KEY FINDINGS – OPERATOR INITIATED FACIAL RECOGNITION

Operator Initiated Facial Recognition is a near-real-time use of facial recognition technology, where an officer takes a photograph of a subject via a mobile device and submits it for immediate search against a reference image database. For each identification search the system returns a short candidate list of the records in the reference image database that best match the submitted probe image.

Recognition accuracy for Operator Initiated Facial Recognition is measured in terms of:

- True-Positive Identification Rate:  $\text{TPIR}(N, R, 0)$  – the proportion of mated identification searches (where the subject has a record in the reference image database) that include the mated reference among the candidates returned.

### 1.3.1 In the evaluation, OIFR always returned the correct reference at Rank 1

For every probe image submitted for OIFR in the evaluation, the correct reference identifier was returned at Rank 1 (i.e., as the top match). This is the best performance possible.

$$\text{TPIR}_{\text{OIFR } 178400, 1, 0} = 100 \%.$$

It follows that TPIR is identical for all demographic subgroups, and with no demographic performance variation in TPIR, performance is equitable.

## 1.4 KEY FINDINGS – LIVE FACIAL RECOGNITION

Live Facial Recognition (LFR) compares a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert.

The recognition accuracy of Live Facial Recognition is measured in terms of:

- True-Positive Identification Rate (TPIR) – the rate of successful recognition when subjects on the watchlist pass through the zone of recognition
- False-Positive Identification Rate (FPIR) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the watchlist pass through the zone of recognition.

TPIR is sometimes referred to as the True Recognition Rate, and FPIR as the False Alert Rate.

TPIR and FPIR depend on the face-match threshold setting of the LFR system. FPIR and, to a lesser extent TPIR, also depend on the number of face images on the watchlist – the number of facial comparisons per subject passing through the zone of recognition, and the potential for a false positive, increases with watchlist size.

#### 1.4.1 A substantial improvement in Live Facial Recognition accuracy

Our tests encompass a range of watchlist sizes and face-match thresholds. For summarising operational performance, we use a face-match threshold of 0.6 which is the default setting of the Neoface facial recognition software. We provide performance figures for two different watchlist sizes: (i) a watchlist of 10,000 reference images, which is close to the size of that previously used in MPS LFR deployments and (ii) a watchlist of 1000 reference images, a size more typical of SWP LFR deployments.

At these settings, combining the data from all five deployments:

| Watchlist size 10,000                              | Watchlist size 1000                                 |
|----------------------------------------------------|-----------------------------------------------------|
| • TPIR <sub>10000, 1, 0.6</sub> = 89 %             | • TPIR <sub>1000, 1, 0.6</sub> = 89 %               |
| • FPIR <sub>10000, 0.6</sub> ≈ 0.017 % (1 in 6000) | • FPIR <sub>1000, 0.6</sub> ≈ 0.002 % (1 in 60,000) |

These accuracy levels are a considerable improvement on that reported [4] for previous versions of the Neoface software. At that time, with watchlist size between 2000 and 4000, averaged over four deployments, TPIR ≈ 72 % and FPIR ≈ 0.1 % (1 in 1000).

#### 1.4.2 The range of variation in True Positive Identification Rate due to demographic effects was the same as that due to environmental effects

At a face-match threshold of 0.6, the variation in TPIR due to demographics of the Test Cohort ranged from a TPIR of 83 % to TPIR of 93 %. The extent of this variation was the same as that due to environmental effects (ranging from TPIR of 83 % to 94 %).

#### 1.4.3 The observed variation in True Positive Identification Rate across gender and ethnicity was not statistically significant

At face-match threshold 0.6, the ethnicity-gender group with the best TPIR was the Asian-Female group, and the poorest TPIR was for the Black-Female group. However, the observed differences in TPIR by gender, by ethnicity, and by ethnicity-gender combined were not statistically significant at the 0.05 significance level. (Statistical significance quantifies whether the observed performance difference is likely due to chance, or due to some underlying factor. Following convention, a 0.05 significance level was set prior to evaluation and analysis of results. Section 4.1 provides further detail on statistical significance.)

#### 1.4.4 Variation of True Positive Identification Rate between age groups

At face-match threshold 0.6, the observed variation in TPIR for the different age groups was statistically significant, TPIR improving with subject age.

The TPIR of 93 % for the oldest quartile (age 42 and over) is significantly higher than the TPIR of 89 % for those in the 20-to-41 age group.

The TPIR of 83 % for the youngest quartile (the under 20's) is significantly lower than the TPIR of 90 % for those aged 20 or over. However, it should be noted that the under-18 portion of the Cohort all attended on the busiest day of the LFR deployments and that, when the zone of recognition was crowded, the TPIR worsened. The lower performance for the under 20's is assessed to be due to both subject and environmental factors, these being a combination of subject age and as a result subject's height, and crowdedness in the zone of recognition leading to shorter subjects being hidden by others from the camera's field of view.

#### 1.4.5 Demographic variation in False Positive Identification Rate is dependent on the face-match threshold

The LFR false positive cases against the 178,000 Filler image watchlist were analysed to determine any significant variation in FPIR between the gender, ethnicity and age demographic groups.

At face-match threshold of 0.64 or higher, there were no false positive identifications, thus at this threshold the FPIR is identically 0.0 for all demographic groups.

At face-match threshold of 0.62, only one Cohort subject had false positive identifications, and, at face-match threshold of 0.60, seven Cohort subjects had false positive identifications. In neither case is the imbalance between demographics statistically significant.

False positive identifications increase at lower face-match thresholds of 0.58 and 0.56 and start to show a statistically significant imbalance between demographics with more Black subjects having a false positive than Asian or White subjects.

#### 1.4.6 Equitability

Under the criteria we have set for equitability (see Section 4):

- TPIR of the system at face-match threshold 0.6 is equitable across gender and ethnicity groups.
- FPIR is equitable between gender and ethnicity and age at face-match threshold 0.6 and above.
- At face-match thresholds lower than 0.6 FPIR equitability will depend on settings of the operational deployment, including size and composition of the watchlist, and the number of crowd subjects passing through the zone of recognition during the deployment.

Given our observations on the demographic variation in FPIR, we would recommend, where operationally possible, the use of a face-match of 0.6 or above to minimise the likelihood of any false positive and adverse impact on equitability.

## 2 EVALUATION OBJECTIVES

This report provides the results of an evaluation of accuracy and equitability of facial recognition technology in three operational use-cases:

- **Live Facial Recognition<sup>2</sup>** (LFR) compares a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert.
- **Retrospective Facial Recognition** (RFR) is a post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.
- **Operator Initiated Facial Recognition** (OIFR) is a near-real-time use of facial recognition technology, where an officer takes a photograph of a subject via a mobile device and submits it for immediate search against a reference image database.

---

<sup>2</sup> In the study the processing of face image data to evaluate LFR, RFR and OIFR was all carried out retrospectively, and omitting any operator involvement in submitting individual images for an identification search, or in adjudication of candidate matches returned by the system. Nevertheless, we shall use the terms LFR and OIFR even though the processing was not 'live', or 'operator initiated'

The objectives of the evaluation are to assess the performance of facial recognition technology in an operational setting in terms of accuracy and equitability related to subject demographics, to add to Law Enforcement's understanding on how their facial recognition algorithms perform, and to provide information on how best to configure FR technology for effective and fair deployment on operational use cases.

The evaluation determines for each operational use case:

- What is the accuracy of the facial recognition algorithms?  
Accuracy of LFR is measured in terms of the True Positive Identification Rate (TPIR) and False Positive Identification Rate (FPIR) as a function of the face-match threshold. Accuracies of RFR and OIFR are measured in terms of the True Positive Identification Rate (TPIR) as a function of the number of top matches returned.
- Equitability is assessed through the consideration of the variations in accuracy for different demographic groups
  - What is the variation in accuracy between the demographic groups?
  - Are the variations in accuracy large enough to be statistically significant?
  - How do demographic variations in accuracy affect outcomes in the operational settings?
- Are demographic performance variations similar over the different operational use cases?
- Are variations in accuracy affected by environmental factors (such as location, crowd density, etc.) and system factors (such as algorithmic thresholds, and composition of watchlist or reference database)?

The evaluation has also collected a ground-truth dataset the UK Law Enforcement Community can use for future testing of other facial recognition algorithms.

### **3 DEMOGRAPHICS**

#### **3.1 DEMOGRAPHIC CATEGORIES**

The demographic factors addressed in this evaluation are: (Self-defined) Ethnicity, Gender, Age and Height.

##### **3.1.1 Ethnicity**

The self-defined ethnicity of Cohort and Filler subjects was classified in accordance with the ONS 5+1 high-level ethnic groups [5]. For sourcing of Cohort subjects, for selection criteria of face images for the Filler reference dataset, and for analysis of performance the grouping of ethnicities used is:

- 'Asian or Asian British' (Bangladeshi, Chinese, Indian, Pakistani, Other Asian)
- 'Black, Black British' (African, Caribbean, Other Black)
- 'White' (English, Welsh, Scottish, Northern Irish, Irish, Gypsy, Roma, Other White)

We shall refer to these high-level groups as 'Asian', 'Black' and 'White' in this report.

These three groups are the largest in the national population (White: 81%, Asian, 9.6%, Black 4.2% [5] ) and consequently the largest in the MPS and SWP custody records and of greatest relevance for policing operations. The remaining two high-level groups 'Mixed or Multiple' and 'Other ethnic group' were intentionally omitted in favour of having higher numbers of Cohort and Filler data for the demographic groups studied.

### 3.1.2 Gender

Gender<sup>3</sup> of the Cohort and Filler subjects was self-declared as Male or Female.

### 3.1.3 Age

To align with the Policing operational use cases for Facial Recognition, the study addressed a broad range of ages. Ages of Cohort subjects were self-declared.

The agencies approached to provide Cohort subjects for the trial were asked (in addition to requirements for gender and ethnicity) to recruit from across the age range 18–65 plus, and to avoid over-representation in the older age ranges. To include under-18's in the Cohort, NPL accepted the offer by MPS to provide Police Cadet volunteers of ages 12 to 18 for one of the deployments.

The selection of Filler data drawn from MPS records is assumed to be representative of the overall subject age profile in the MPS custody records. In the final datasets, the age profile of Cohort and Filler was quite similar in terms of interquartile ranges. For analysis of the differences in performance between age groups, we divided Cohort subjects into quartiles by age, from the youngest quartile to the oldest quartile.

### 3.1.4 Height

Height data was recorded for the Cohort as it was thought possible that occlusion of one subject behind another could adversely affect face detection, and this would be a more likely occurrence for the shortest subjects than for the tallest.

## 4 ASSESSING EQUITABILITY

The evaluation is assessing facial recognition accuracy, variations in performance for different demographics, and equitability between demographics in operational systems. Demographic variation in accuracy performance may be more easily observable at settings outside the normal operational parameters, hence our use of a Filler dataset to allow a watchlist much larger than those of typical LFR deployments. However, equitability must be assessed at typical operational settings.

For consideration of equitability in operational LFR deployments we hypothesise two watchlists of size and demographic composition to be typical for MPS and SWP operational deployments. The first has 10,000 face images, the second 1000 face images, and in both cases the composition of the watchlist can be expected to be proportional to the number of arrests in 2020/2021 by MPS and SWP respectively [6].

To scale results of larger watchlist (size  $c \times N$ ) to a smaller watchlist (size  $N$ ) we note that, provided  $\text{FPIR}(N, T)$  is small:

$$\begin{aligned} \text{TPIR}(c \times N, 1, T) &\approx \text{TPIR}(N, 1, T) \text{ and} \\ \text{FPIR}(c \times N, T) &\approx c \times \text{FPIR}(N, T). \end{aligned}$$

Equitability between demographics requires that, in the operational setting, the outcomes for the subjects (i.e., recognition rates and false alert rates) should be broadly equivalent for demographics considered.

---

<sup>3</sup> **Gender:** classification as male, female or another category based on social, cultural or behavioural factors. (Gender is generally determined through self-declaration or self-presentation and may change over time.)

We cannot require exact equivalence as, even when there is no demographic variation in performance, due to the statistical nature of biometrics small deviations in observed performance must be expected. Thus, in assessing whether a system is equitable, criteria are needed for broad equivalence of performance figures.

In this study we use the following criteria for determining equitability:

- a) The system is performing equitably if there is no variation in performance between demographic groups (e.g., when there are no false positives at the face-match threshold applied).
- b) The system is performing equitably if the variation in performance between demographic groups is not statistically significant.
- c) The system is performing equitably if the variation in performance between demographics is inconsequential in the operational system (e.g., if there is virtually no difference in outcomes for the different demographics).

#### 4.1 STATISTICAL SIGNIFICANCE

Statistical significance quantifies whether the observed performance difference is likely due to chance, or due to some underlying factor of interest. For testing of statistical significance in the evaluation, we use the conventional significance level 0.05 (5%).

The significance level relates to the probability of falsely rejecting the 'null' hypothesis that there is no underlying difference in performance rates.

Note that testing for performance variation over different demographic attributes involves multiple hypothesis tests. A multiplicity of tests each at 5% significance level can increase the probability of rejecting the null hypothesis to a value much higher than 5%. There are methods to address this issue by requiring stricter significance thresholds for each individual test (however this increases the chance of missing a demographic effect). Such methods were NOT applied in this evaluation.

### 5 OUTLINE OF METHODOLOGY AND DATA

The tests conducted emulate the operational LFR, RFR and OIFR use cases.

A set of facial photographs were taken of a Cohort of subjects in a variety of settings including 'Custody-style' images captured in accordance with the Police Standard for Still Digital Image Capture of Facial Images [7]. The custody-style images were used for enrolling custody subjects onto a LFR watchlist, and facial image reference dataset for RFR and OIFR.

Video featuring Cohort subjects was collected alongside an operational LFR deployment and so reflects typical operational conditions. The behaviour of Cohort subjects seeded into the crowd was also consistent with normal crowd behaviour (other than being under instruction to ensure that they did pass through the zone of recognition, and to have a barcode scanned after going through the zone of recognition to log timings, and to walk through the zone of recognition the requisite number of times).

The following differences between the evaluation conditions and normal operational use should be noted.

- a) For purposes of the evaluation, the watchlist used for testing of Live Facial Recognition was an order of magnitude larger than typical for an MPS LFR deployment. The watchlist contained nearly 180,000 face images, which is about 20 times the size of any watchlist used operationally to date. The increased watchlist size was to help ensure there would be sufficient data on true and false positive alerts to draw meaningful (statistically significant) conclusions regarding demographic differences in performance.
- b) To address the purposes of the evaluation in assessing demographic variation in performance, the Filler and Cohort watchlists comprised an approximately equal number of face images for males and females of Asian, Black, and White ethnicities. In operational deployments the demographic balance of the watchlist would be different, and more likely to reflect the demographic balance in society, or of images in the MPS or SWP Custody Image Systems.
- c) The facial recognition algorithms were configured to run in a bulk processing mode without the need for operator involvement or interaction during the process. The volume of data makes it impractical to involve the operator in processing each image, though this might be the case in operational use of RFR or OIFR.
- d) In particular, the settings of the systems were not dynamically adjusted by test staff during running as conditions of facial images and video footage varied.
- e) There was no operator or test staff adjudication of candidate matches returned by the system; the effects of such adjudication are outside the scope of the study.
- f) The LFR video was not 'live stream' video but had been saved as mp4 files. At times, artefacts of compression were noticeable in the videos. Such artefacts can affect face image quality and may have had a negative impact on the accuracy of facial recognition compared with uncompressed video used for live deployments.

## 5.1 COHORT DATA SUBJECTS

A Cohort of test subjects meeting the demographic requirements for the study were recruited via acting extras agencies and an additional under-18 Cohort of test subjects were provided from MPS Police Cadet volunteers.

We have used the demographic details that subjects provided when they completed our demographics form; in some cases this was different to that stated by the supplying agency. A summary of the details is shown in Table 1. The number and demographic mix of the Cohort data subjects is sufficient to test equitability between Male/Female gender, Asian/Black/White ethnicity, and Age groups.

**Table 1 — Summary of Cohort composition**

| <b>Cohort composition: 405 Data subjects</b>  |                            |               |             |
|-----------------------------------------------|----------------------------|---------------|-------------|
|                                               |                            | <b>Female</b> | <b>Male</b> |
| Self-defined ethnicity based on ONS 5+1 codes | Asian (A1, A2, A3, A4, A9) | 53            | 45          |
|                                               | Black (B1, B2, B9)         | 60            | 51          |
|                                               | White (W1, W2, W3, W9)     | 84            | 86          |
|                                               | Mixed and Other            | 8             | 16          |
| Age                                           | Age range                  | 12 - 76 years |             |
|                                               | Lower Quartile             | 20 years      |             |
|                                               | Median                     | 30 years      |             |
|                                               | Upper Quartile             | 42 years      |             |



## 5.2 FACIAL IMAGES OF COHORT

A set of facial photographs was taken of each Cohort subject alongside the MPS and SWP deployments of Live Facial Recognition. The photographs were taken in a variety of settings as summarised in Table 2. Measurement of RFR and OIFR accuracy is based on the Cohort probe and reference images as listed in the table.

**Table 2 — Summary of types of reference and probe images used in the study**

| Image type                                                                                                                                                                                                                                                                                                              | Uses                                                                                               | Camera / Location                                           | Number of images |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------|------------------|
| Custody style <sup>4</sup><br>Image of the full head with all hair, neck, shoulders and ears.<br>Subject facing square to the camera, looking directly at camera.<br>Diffuse lighting to provide uniform illumination across the face without hot spots or shadows.<br>Plain flat background with an 18% shade of grey. | Enrolment of reference image for watchlist or reference image database<br><br>Probe images for RFR | Canon EOS850D<br>Indoor                                     | 686              |
| OIFR<br>A facial image taken on a mobile phone (same model as used by SWP for OIFR).<br>In cases where the image is out-of-focus, there is motion blur, or the subject’s eyes were closed a further image would be taken.                                                                                               | Probe images for OIFR                                                                              | Samsung XcoverPro<br>Indoor                                 | 567              |
|                                                                                                                                                                                                                                                                                                                         | Probe images for RFR                                                                               | Samsung XcoverPro<br>Outdoor<br>Some images at LFR location | 576              |
| Selfie<br>Mobile phone image taken by Cohort subject.<br>Subject permitted to pose as they wished for the photo.<br>A neutral expression was not required, and the subject did not need to pose ‘square to the camera’                                                                                                  | Probe images for RFR                                                                               | Motorola G(60)s<br>Indoor                                   | 570              |
|                                                                                                                                                                                                                                                                                                                         |                                                                                                    | Motorola G(60)s<br>Outdoor                                  | 453              |
| Ad hoc digital camera image<br>Camera image of the subject taken either inside or outside.<br>Uncontrolled conditions and background.<br>No flash or supplementary lighting.<br>Some of the ad-hoc outdoor photos were taken at the LFR location.                                                                       | Probe images for RFR                                                                               | Nikon D40<br>Indoor                                         | 506              |
|                                                                                                                                                                                                                                                                                                                         |                                                                                                    | Nikon 1 J5<br>Outdoor<br>Some images at LFR location        | 582              |
| <b>Note:</b><br>Images taken with Cohort subject wearing facemasks are excluded.<br>(Performance and equitability for subjects wearing facemasks not assessed in this study).                                                                                                                                           |                                                                                                    |                                                             |                  |

<sup>4</sup> Conformant to "Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images" Version 2, 2007

### 5.3 VIDEO FROM LIVE FACIAL RECOGNITION DEPLOYMENTS

Measurement of LFR accuracy is based on the Cohort identification transactions (the 'recognition opportunities' as Cohort subjects walk through the zone of recognition of the LFR system). Details of LFR deployments are shown in Table 3.

**Table 3 — Summary of LFR deployments with seeded Cohort subjects**

| Date        | Location                  | Duration  | Estimated number of crowd subjects |
|-------------|---------------------------|-----------|------------------------------------|
| 7 Jul 2022  | London, Oxford Street     | 7 hours   | 24000                              |
| 14 Jul 2022 | London, Oxford Street     | 8 hours   | 35000                              |
| 16 Jul 2022 | London, Oxford Street     | 8 hours   | 38000                              |
| 28 Jul 2022 | London, Piccadilly Circus | 7 hours   | 28000                              |
| 13 Aug 2022 | Cardiff, Queen Street     | 4.5 hours | 7000                               |

Weather conditions were quite similar during the five deployments, precluding analysis of weather effects. All days were bright and sunny, and several Cohort subjects wore sunhats and sunglasses in keeping with the conditions. August 13 was exceptionally hot (peak temperature: 33 °C).

Video was collected from two camera systems spanning the zone of recognition of the LFR deployment except for the afternoon of 13 August when a single camera was used.

The number of crowd subjects was estimated by taking a one-minute sample of each 30-minute video and combining contemporaneous footage from both cameras. Staff counted the number of subjects walking towards the camera in each sample video to estimate the number of crowd subjects seen by the LFR camera per minute. Multiplying by 30 gives the number of crowd subjects for the pair of videos, and the daily estimate sums the numbers for that day's videos.

The estimated number of subjects per minute is also used as a measure of how congested the zone of recognition was at the times the Cohort recognition opportunities were recorded. (The actual numbers in the zone of recognition would need to take into account (i) that the crowd walks both towards and away from the camera, and (ii) the time duration it takes for someone in the crowd to move through the zone of recognition. When the zone of recognition was very busy, it took more time for subjects to walk through.

## 5.4 FILLER FACIAL IMAGES

A Filler dataset was used to provide a large watchlist or reference dataset for evaluating LFR, RFR and OIFR performance. The demographic composition of the dataset is shown in Table 4.

**Table 4 — Summary of Filler facial image set**

| <b>Filler dataset from MPS holdings: ~ 178,000 facial images from ~ 116,000 individuals</b> |                            |                       |             |
|---------------------------------------------------------------------------------------------|----------------------------|-----------------------|-------------|
|                                                                                             |                            | <b>Female</b>         | <b>Male</b> |
| Self-defined ethnicity based on ONS 5+1 codes                                               | Asian (A1, A2, A3, A4, A9) | ~ 30 000              | ~ 30 000    |
|                                                                                             | Black (B1, B2, B9)         | ~ 30 000              | ~ 30 000    |
|                                                                                             | White (W1, W2, W3, W9)     | ~ 30 000              | ~ 30 000    |
| Age at date image taken                                                                     | Age Range <sup>5</sup>     | Approx. 12 - 76 years |             |
|                                                                                             | Age Lower Quartile         | 22 years              |             |
|                                                                                             | Age Median                 | 31 years              |             |
|                                                                                             | Age Upper Quartile         | 41 years              |             |

The Filler dataset has approximately 180,000 face images: 30,000 for each of the Gender/Ethnicity groups shown. Approximately 2000 of the supplied images could not be enrolled at the default settings (e.g., those with a profile rather than frontal face image). We did not attempt to adjust the settings to enrol the failed cases; in previous deployments it has been observed that poor quality watchlist images were prone to increasing the incidence of false alerts.

Each Filler image corresponds to a custody record, and the Filler dataset contains multiple images for some individuals who have multiple custody records. Guidance on watchlist composition [7] suggests that if multiple different images of a subject are available, consideration be given to including these in the watchlist to improve the likelihood of a match. Thus, the inclusion of multiple images for some individuals is not atypical of the operational use case.

## 6 EVALUATION RESULTS – RETROSPECTIVE FACIAL RECOGNITION

### 6.1 METHODOLOGY

#### 6.1.1 Comparison program

To automate the testing of RFR and OIFR, NEC provided a programme to NPL's specification that enabled batch processing of identification searches using the Neoface V4 algorithm without requiring operator involvement. The program uses the Neoface facial recognition server to perform an identification search of each probe image in a specified directory against a reference image database or watchlist, and logs the identifiers of the returned candidates, and the corresponding comparison scores.

#### 6.1.2 Reference image database and Probe images

The reference image dataset for RFR combines (i) an enrolled watchlist of Custody-style Cohort images, and (ii) the enrolled Filler dataset of custody images.

<sup>5</sup> Age range for Filler dataset taken as the 0.1% - 99.9% percentiles

The probe images used for RFR were the full set of facial images of the Cohort subjects collected in conjunction with the LFR deployments. The image types are listed in Table 2.

To facilitate the use of the matching programme, the collected images were cropped and downsized. Cropping was necessary as the programme for batch processing cannot handle cases where multiple faces appear within an image. The Neoface system itself can handle this situation, but the process requires operator interaction in selecting the faces of interest. Some of the face images were cropped quite tightly to avoid other nearby faces in the background.

Given the size of the Filler dataset, there was a chance that a Cohort subject could also feature in the Filler dataset. This could risk a correct match between Cohort subject and their Filler image being counted as a false positive. (It would also complicate handling of any Cohort requests to have their data removed from the evaluation datasets.) The issue was addressed by checking cases where a Cohort-to-Filler comparison score was beyond the typical range for 'non-mated comparisons' and within the range for 'mated comparison'. In such cases if the Cohort and Filler metadata agree the Filler image would be removed from the Filler datasets. Six checks were made, and four Filler subjects were removed.

### 6.1.3 Running RFR

For RFR the matching process was configured to return for each probe the comparison score and candidate ID of the top 200 matches in the reference image database. (This would allow reporting of the RFR TPIR for the correct reference being returned with the top R matches for  $R = 1$  to  $R = 200$  as per the test strategy).

## 6.2 ACCURACY

For every probe image submitted for RFR, the correct reference was returned at Rank 1 (i.e., as the top match). This is the best possible performance<sup>6</sup>.

$$\text{TPIR}_{\text{RFR } 178400, 1, 0} = 100 \text{ \%}.$$

It follows that TPIR is identical at 100 % for all demographic subsets of the submitted probe images and, with no demographic variation in TPIR, the performance is equitable.

It also follows that  $\text{TPIR}_{178400, 1, 0} = 100 \text{ \%}$  for all the different types of probe image, and in particular the images taken with the OIFR device.

The result also suggests that in the operational use of RFR, the number of top-matching candidates returned for operator adjudication could be somewhat smaller than 200 (say 10 rather than 200).

### 6.3 LOW SCORING MATED COMPARISONS & HIGH-SCORING NON-MATED COMPARISONS

Excluding matches between identical twins (addressed in Section 6.4), in the full set of RFR identification searches the highest non-mated comparison score was 0.653, and there were ten non-mated comparison scores above 0.60 (arising from probes images of four Cohort subjects). The probes of one Cohort subject had matches above score 0.6 against five different Filler subjects. This particular Cohort subject is clearly an outlier, but we have not

---

<sup>6</sup> All probes are recognised at Rank 1, and therefore no breakdown is given by subset for different image types, different Cohort demographics, different rank values.

been able to isolate a specific reason behind this anomaly. (In biometric systems it is not uncommon that a few subjects are more prone to false-matches than others [8]).

Thirteen RFR identification searches (out of approximately 4000) returned mated comparison score below the 0.653 highest non-mated score. The probe images in these cases generally met configured face detection parameters but were less than ideal. Typical issues being reflections in glasses, shadows over the eyes, glasses' frames over the eyes. Despite these issues the subjects were still correctly recognised at Rank 1.

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.

## 6.4 IDENTICAL TWINS

In the Cohort there was a pair of identical twins; identical twins are known to be a challenging case for facial recognition. In the running of RFR and OIFR each twin was always correctly recognised at Rank 1, and their sibling was returned as the Rank-2 candidate. The non-mated comparison scores between the identical twins were (unsurprisingly) higher than that usual for non-mated comparison scores, and within the range 0.7 to 0.8 of typical for mated comparison scores.

In running of LFR, both of the identical twins were enrolled onto the Cohort watchlist; they were always recognised correctly and there were no cases of one of the twins being incorrectly recognised as the other.

There was also a pair of fraternal twins in the Cohort. RFR and OIFR non-mated comparison scores between the fraternal twins were within the usual range for non-mated scores. Neither twin featured as a Rank-2 candidate for their sibling.

## 7 EVALUATION RESULTS – OPERATOR INITIATED FACIAL RECOGNITION

### 7.1 METHODOLOGY

The methodology for evaluating OIFR is very similar to that for RFR. The differences being that:

- a) Only the 'OIFR-style' images taken with the Samsung XcoverPro mobile phone were used as Probe Images. The reference image database combines the enrolled Filler dataset, and the enrolled 'Custody-style' Cohort images as in the case for RFR.
- b) The NEC matching program was configured to return just the top 6 matches.

### 7.2 ACCURACY

For every probe image submitted for OIFR the correct reference was returned at Rank 1 (i.e., as the top match). This is the best possible performance.

$$TPIR_{OIFR, 178\ 400, 1, 0} = 100 \%$$

It follows that the OIFR TPIR is identical at 100 % for all demographic groups and there is no demographic variation in TPIR and the OIFR TPIR performance is equitable.

### 7.3 LOW SCORING MATED COMPARISONS & HIGH-SCORING NON-MATED COMPARISONS

Excluding matches between identical twins, in the full set of OIFR identification searches the highest non-mated comparison score was 0.653. Five OIFR identification searches returned the correct reference image at Rank 1, though with a mated comparison score below this value (0.55-0.64). In four of the cases, features of the face and eyes were obscured by reflections in the subjects' glasses. In the fifth case due to the angle of the sun there were dark shadows in the eye-sockets. In the operational OIFR use-case the operator taking the photograph might seek to take a further image of the subject when such face-image quality issues arise.

The OIFR use case currently operates without a face-match threshold, but had a face-match threshold of 0.66 been set, then with our OIFR probe images, and with the Cohort enrolled, all but these 5 cases would have been recognised at Rank 1, and if the Cohort subject is not enrolled onto the reference image database, no candidates would have been returned for the subject (except in the case of the identical twins).

## 8 EVALUATION RESULTS – LIVE FACIAL RECOGNITION

### 8.1 METHODOLOGY

#### 8.1.1 Collection of LFR video featuring Cohort

Cohort subjects were seeded into to the Crowd flow over the course of the operational LFR deployments. These deployments were running with an operational watchlist, which did not feature the Cohort.

At the street location of the LFR system, start and endpoints for the repeat walks by Cohort subjects through the zone of recognition (Recognition Opportunities) were selected such that a round trip through the zone of recognition back to the start point should take at least one minute. To prevent multiple alerts from a single recognition opportunity, the Neoface algorithm is configured such that once an individual is alerted, a second alert within 30 seconds is ignored.

To count and log timings of the Cohort recognition opportunities, each Cohort subject had been issued with a lanyard and badge showing their unique reference number (URN) as a number and a barcode. Scanning the barcodes logged the URN and time of scan to a spreadsheet.

At the LFR location Cohort subjects were briefed:

- a) To ensure that they walked through the zone of recognition of the LFR systems.
- b) To walk as they would normally; there was not a need to look directly at the camera, but not to be looking down at their mobile phone while walking towards the camera.<sup>7</sup>
- c) To avoid bunching into one large group. It was suggested that they might walk in pairs and allowed to converse.

---

<sup>7</sup> While it is operationally realistic that some of the crowd intentionally or accidentally avoid showing their face to the LFR system, the focus of the evaluation was on the accuracy and equitability of the LFR for those faces processed by the system.

- d) Cohort subjects were instructed to have their lanyard-badge barcode scanned for each walk through the zone of recognition.

We did not prohibit or suggest the wearing of caps, sunhats or sunglasses, glasses. The wearing of sunglasses and hats was typical for the non-cohort public passing the LFR system.

#### 8.1.2 Enrolment of Cohort and Filler watchlists

In conjunction with the LFR deployment, face images of the types listed in Table 2 were collected from the Cohort. These included 'custody image' style photographs. For subjects that normally wear glasses, photographs were taken both with and without glasses. Enrolment of Cohort subjects onto a Cohort watchlist used the custody-style photographs without glasses. These photographs were taken at a high resolution (6000 x 4000 pixels, with approximately 700 pixels between the eyes) and were cropped and downsized (to approximately 200 pixels between eyes) to meet requirements for watchlist enrolment (max 300 pixels between eyes).

A Filler watchlist was enrolled of the full Filler dataset. (Filler images averaged approximately 130 pixels between eyes.)

#### 8.1.3 Offline running of LFR

The LFR video footage was provided after the deployment as a series of 30 minute .mp4 files from each camera. This allowed the video to be run retrospectively on the Neoface V4 system replicating the live video stream but using the Cohort and Filler watchlists.

The collected LFR videos were run against Cohort and Filler watchlists at a range of face-match thresholds 0.56 to 0.64 spanning the Neoface default setting of 0.60.

In addition to the face-match threshold, the algorithm has configurable settings controlling face detection, (based on proprietary measures for face reliability, face quality score, face frontal score, minimum and maximum pixels between eye centres). Good quality frontal face images of sufficient size give the most accurate identification results, but the strictest settings may mean that some faces go undetected by the system. Relaxing the criteria for face detection increases the number of faces to be processed for comparison which may improve the true recognition rate but may also increase the false match rate. The increased computational workload may mean that fewer frames of video can be processed in real-time operation.

#### 8.1.4 Face detection parameters

In this evaluation we first ran the LFR videos without adjusting face detection thresholds from the Neoface software default settings. Our results at these settings showed an anomaly in the recognition performance at the Cardiff deployment. The extreme heat on 13<sup>th</sup> August caused the LFR cameras to malfunction. In order to continue the deployment with minimum delay, the failing system was replaced with a second single camera system but without the normal processes of optimising camera and zone of recognition settings. Our initial results showed a significantly lower True Recognition Rate for the replacement system, and inspection of the video footage showed that face images were smaller and less 'frontal' than before the change. Accordingly, the affected LFR videos were re-run with face detection settings adjusted to allow for face images of a smaller size and with greater divergence from a frontal pose. The change improved accuracy to the levels prior to the camera malfunction.

Investigation into the effects of altering face detection settings was also carried out for processing the LFR video of the four London deployments. Here the potential values for 'Face reliability score' and 'Face frontal score' were limited by requirements for real-time operation on the servers used. The changes made led to an improvement in TPIR. However, we observed that some of the additional faces found are of poorer quality and more liable to falsely match, increasing the FPIR.

#### 8.1.5 Determination of performance

For determination of the False Positive Identification Rate, LFR videos were run against the Filler watchlist emulating the Live Facial Recognition process but using the saved videos in place of the live video feed. The resulting 'Match Details Report' produced by the system lists all the Crowd and Cohort matches against the Filler watchlist at the threshold setting. The Match Details Report was inspected to determine which of the matches are of a Cohort subject matched to a Filler reference image. This determination was aided by:

- a) the barcode scanned timings of Cohort recognition opportunities,
- b) timing information derived from the Match Details Report,
- c) images of the Cohort taken on the street,
- d) the green lanyard with URN badge normally visible in the captured face image shown in the Match Details Report.

Matches between Crowd and Filler were disregarded in the evaluation, as no 'ground truth' is available to establish which of these matches are correct.

For determination of the True Positive Identification Rate, LFR videos were run against the combined Filler and Cohort watchlists. The recognitions logged in the Match Details Report were then compared against the log of barcode scans to determine how many of Cohort subject's recognition opportunities resulted in their correct recognition, and how many times they were missed.



## 8.2 ACCURACY

Table 5 — TPIR and FPIR by threshold setting

| Face-match threshold                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Face detection settings | Observed TPIR                | Observed FPIR             | FPIR anticipated under operational measures: Watchlist 10k | FPIR anticipated under operational measures: Watchlist: 1k |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------|---------------------------|------------------------------------------------------------|------------------------------------------------------------|
| T                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         | TPIR <sub>178400, 1, T</sub> | FPIR <sub>178000, T</sub> | FPIR <sub>10000, T</sub>                                   | FPIR <sub>1000, T</sub>                                    |
| 0.64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (a)                     | 79 %                         | 0.00 %                    | < 0.004 %                                                  | < 0.001 %                                                  |
| 0.62                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (a)                     | 82 %                         | 0.05 %                    | < 0.004 %                                                  | < 0.001 %                                                  |
| 0.60                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (a)                     | 85 %                         | 0.25 %                    | 0.014 %                                                    | 0.002 %                                                    |
| 0.60                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (b)                     | 89 %                         | 0.30 %                    | 0.017 %                                                    | 0.002 %                                                    |
| 0.58                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (a)                     | 88 %                         | 0.48 %                    | 0.027 %                                                    | 0.003 %                                                    |
| 0.56                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (a)                     | 94 %                         | 1.15 %                    | 0.065 %                                                    | 0.007 %                                                    |
| <b>Notes:</b><br>TPIR <sub>178400, 1, T</sub> based on 4000 mated recognition opportunities<br>FPIR <sub>178000, T</sub> based on 4000 non-mated recognition opportunities<br>FPIR <sub>10000, T</sub> & FPIR <sub>1000, T</sub> estimates based on scaling results on the 178k watchlist to 10k and 1k<br><br><b>Face detection settings (a)</b><br>London deployments: Face Reliability 0.80, Face Frontal Score: 0.4, Eyes Min Distance 60, Face Roll 30<br>Cardiff deployment: Face Reliability 0.80, Face Frontal Score: 0.3, Eyes Min Distance 40, Face Roll 30<br><b>Face detection settings (b)</b><br>London deployments: Face Reliability 0.75, Face Frontal Score: 0.35, Eyes Min Distance 60, Face Roll 30<br>Cardiff deployment: Face Reliability 0.80, Face Frontal Score: 0.3, Eyes Min Distance 40, Face Roll 30 |                         |                              |                           |                                                            |                                                            |

Table 5 shows the observed True Positive and False Positive Identification Rates, aggregated over the video from all five LFR deployments, and at face-match thresholds ranging from 0.56 to 0.64. Over this threshold range the True Recognition Rate ranges from 79% to 94%.

At a face-match threshold of 0.64, the software produced no false positives against the watchlist of 178,000 Filler images. At threshold 0.62, two non-mated recognition opportunities (by the same individual) gave a false positive. At threshold 0.60, ten non-mated recognition opportunities generated false positives (increasing to twelve with the revised face detection settings).

The evaluation watchlist of 178,000 images is much larger than that used in operational deployments: all MPS LFR deployments to date have used watchlists smaller than 10000. With a watchlist of 10,000 rather than 178,000 face images the FPIR should reduce by a factor of 17.8. Thus, in an operational setting with a watchlist of 10,000 face images and a face-match threshold of 0.60, the anticipated False Alert Rate (FPIR<sub>10000, 0.6</sub>) is 0.017 %<sup>8</sup> (approximately 1 in 6000), and at face-match threshold of 0.62 the anticipated False Alert Rate (FPIR<sub>10000, 0.62</sub>) is 0.004 % (approximately 1 in 25000). This would equate to one or two false alerts per LFR deployment day were the crowd numbers similar to those of the deployments used in this study.

These accuracy levels are a considerable improvement on that reported for previous versions of the Neoface software (with watchlist size between 2000 and 4000, averaged over four deployments, TPIR ≈ 72 % and FPIR ≈ 0.1 % (1 in 1000). [5]).

<sup>8</sup> Sometimes it is easier to comprehend FPIR when expressed as a ratio e.g., “1 in 6000” than when expressed as a percentage, in this case “0.017%”.  $x\% = 1 \text{ in } (100 \div x)$

## 8.3 DEMOGRAPHIC VARIATION IN FALSE POSITIVE IDENTIFICATION RATE

**Table 6 — Number of Cohort subjects with false positive by Gender, Ethnicity & Age**

| Face-match threshold<br>Face-detection settings                             | FPIR   | Female | Male | Asian | Black | White | Age<br><21 | Age<br>21-30 | Age<br>31-42 | Age<br>>42 |
|-----------------------------------------------------------------------------|--------|--------|------|-------|-------|-------|------------|--------------|--------------|------------|
| 0.64 (a)                                                                    | 0.00 % | 0      | 0    | 0     | 0     | 0     | 0          | 0            | 0            | 0          |
| 0.62 (a)                                                                    | 0.05 % | 1      | 0    | 0     | 1     | 0     | 0          | 1            | 0            | 0          |
| 0.60 (a)                                                                    | 0.25 % | 2      | 4    | 2     | 4     | 0     | 0          | 5            | 1            | 0          |
| 0.60 (b)                                                                    | 0.30 % | 2      | 5    | 4     | 3     | 0     | 0          | 7            | 0            | 0          |
| 0.58 (a)                                                                    | 0.48 % | 7      | 8    | 4     | 11    | 0     | 2          | 9            | 3            | 1          |
| 0.56 (a)                                                                    | 1.15 % | 16     | 17   | 8     | 22    | 3     | 7          | 18           | 7            | 1          |
| Recognition opportunities:<br>gender, ethnicity & age<br>balance            |        | 51%    | 49%  | 26%   | 29%   | 45%   | 26%        | 26%          | 24%          | 24%        |
| <b>Notes:</b><br>Watchlist size: 178,000<br>Recognition opportunities: 4000 |        |        |      |       |       |       |            |              |              |            |

Table 6 shows the demographic of the Cohort subjects falsely matched to Filler images at the tested face-match thresholds.

At face-match thresholds of 0.64 and higher there were no false positives.

At face-match thresholds of 0.62 and 0.60 the number of subjects with a false positive is small, and a statistically significant imbalance between demographics is not shown.

At face-match thresholds of 0.58 and 0.56 we observe that false positives are not uniform between demographic groups. In particular, the number of false positives is disproportionately higher for Black subjects than for Asian or White subjects; this demographic variation in  $FPIR_{178000, 0.56}$  is statistically significant ( $p < 0.01$ ).

## 8.4 DEMOGRAPHIC VARIATION IN TRUE POSITIVE IDENTIFICATION RATE

Table 7 — True Positive Identification Rate by demographics and other factors

| Demographic                   | TPIR | Statistically Significant | p-value     | Other factors                           | TPIR | Statistically Significant | p-value     |
|-------------------------------|------|---------------------------|-------------|-----------------------------------------|------|---------------------------|-------------|
| <b>All Cohort subjects</b>    | 89 % |                           |             |                                         |      |                           |             |
| <b>Gender</b>                 |      |                           |             | <b>LFR Deployment</b>                   |      |                           |             |
| Female                        | 87%  | no                        |             | Jul 07 – Oxford St                      | 90 % | no                        |             |
| Male                          | 90 % | no                        |             | Jul 14 – Oxford St                      | 91 % | no                        |             |
| <b>Ethnicity</b>              |      |                           |             | Jul 16 – Oxford St                      | 83 % | Yes                       | $p = 0.017$ |
| Asian                         | 91 % | no                        |             | Jul 28 – Piccadilly                     | 89 % | no                        |             |
| Black                         | 86 % | no                        | $p = 0.144$ | Aug 13 – Cardiff                        | 94 % | Yes                       | $p = 0.003$ |
| White                         | 89 % | no                        |             | <b>Crowd density</b>                    |      |                           |             |
| <b>Ethnicity &amp; Gender</b> |      |                           |             | People walking toward camera per minute |      |                           |             |
| Asian – Female                | 91 % | no                        |             | < 71                                    | 91 % | Yes                       | $p = 0.005$ |
| Asian – Male                  | 90 % | no                        | $p = 0.051$ | > 70                                    | 85 % | Yes                       | $p = 0.005$ |
| Black – Female                | 83 % | no                        |             |                                         |      |                           |             |
| Black – Male                  | 90 % | no                        |             |                                         |      |                           |             |
| White – Female                | 89 % | no                        |             |                                         |      |                           |             |
| White – Male                  | 88 % | no                        |             |                                         |      |                           |             |
| <b>Age</b>                    |      |                           |             |                                         |      |                           |             |
| < 21 years                    | 84 % | Yes                       | $p = 0.037$ |                                         |      |                           |             |
| 21-30 years                   | 87 % | no                        |             |                                         |      |                           |             |
| 31-42 years                   | 91 % | no                        |             |                                         |      |                           |             |
| > 42 years                    | 93 % | Yes                       | $p = 0.009$ |                                         |      |                           |             |
| <b>Height</b>                 |      |                           |             |                                         |      |                           |             |
| < 164 cm                      | 86 % | no                        | $p = 0.157$ |                                         |      |                           |             |
| 164-170 cm                    | 87 % | no                        |             |                                         |      |                           |             |
| 171-178 cm                    | 90 % | no                        |             |                                         |      |                           |             |
| > 178 cm                      | 91 % | no                        | $p = 0.116$ |                                         |      |                           |             |

**Notes:**TPIR = TPIR<sub>178400, 1, 0.60</sub>**Configuration parameter settings:**

Face-match threshold: 0.60

Face Reliability: 0.75 (London) 0.8 (Cardiff)

Face Frontal Score: 0.35 (London) 0.3 (Cardiff)

Eyes Min Distance: 60 (London) 40 (Cardiff)

Face Roll: 30

Table 7 shows the observed variation in the True Recognition Rate for different demographic subgroups and other factors of interest at a face-match threshold of 0.6. A *t*-test (Welch's unequal variance *t*-test) was used to determine whether demographic differences in performance are statistically significant at the 0.05 significance level. Table 7 also shows computed *p*-values for cases where the difference (higher or lower TPIR) is statistically significant, cases close to the 0.05 significance threshold, and outliers in each demographic or environmental category.

## 8.4.1 Ethnicity and Gender

At a face-match threshold of 0.6, the ethnicity-gender group with the best TPIR was the Asian-Female group, and the poorest TPIR was for the Black-Female group. However, the observed differences in TPIR by gender, by ethnicity, and by ethnicity & gender combined were not statistically significant at the 0.05 significance level.

- The demographic variation in TPIR between Black females ( $M = 0.83$ ,  $SD = 0.26$ ) and the other ethnicity-gender demographics ( $M = 0.90$ ;  $SD = 0.20$ ) was not significant ( $t(71.7) = 1.98$ ;  $p = .051$ )

### 8.4.2 Age

The observed TPIR was significantly lower for those aged 20 or below ( $M = 0.84$ ;  $SD = 0.25$ ), than for those aged 21 and over ( $M = 0.90$ ;  $SD = 0.19$ ), ( $t(143.1) = 2.11$ ;  $p = .037$ ). However, this age effect on performance is confounded with the effect of congestion in the Zone of Recognition. Most of the subjects in the under-20 age category were Police Cadet volunteers attending the deployment on 16 July. This was also the deployment in which the zone of recognition was the most congested. We discuss this further in Section 8.4.3.

The observed TPIR for those aged over 42 ( $M = 0.93$ ;  $SD = 0.17$ ) was significantly higher than for those aged between 21 and 42 ( $M = 0.89$ ;  $SD = 0.2$ ), ( $t(231.9) = 2.11$ ;  $p = 0.036$ ).

### 8.4.3 Crowdedness of zone of recognition, and subject height

The observed TPIR when crowd density was above 70 ( $M = 0.85$ ,  $SD = 0.25$ ) was significantly higher than that when crowd density was below 70 ( $M = 0.91$ ,  $SD = 0.15$ ), ( $t(315.0) = 2.86$ ,  $p = 0.005$ ).

It also appears that subject height is an important factor when the zone of recognition is crowded. The supposition is that shorter subjects are more likely than taller subjects to be occluded or partly occluded in the camera field of view when the zone of recognition is crowded.

On the most crowded day 16 July, the observed TPIR for subjects shorter than 170 cm (median height) ( $M = 0.77$ ,  $SD = 0.31$ ) was significantly lower than that for subjects taller than 170 cm ( $M = 0.91$ ,  $SD = 0.17$ ), ( $t(86.5) = 2.69$ ,  $p = 0.009$ ). The lower performance of the under 20's is therefore assessed to be due to both demographic and environmental factors, these being a combination of subject age and as a result subject height, and crowdedness in the zone of recognition.

## 9 DISCUSSION

### 9.1 ARE DEMOGRAPHIC PERFORMANCE VARIATIONS SIMILAR FOR LFR, RFR AND OIFR?

The same face matching algorithm is used for LFR, RFR, and OIFR and in the evaluation using the same Cohort individuals and same reference image sets, the findings on demographic performance variation are very similar. Due to the similarity, it may be possible to use the bulk RFR software and a set of Cohort data to assess the FPIR equitability of a specific watchlist prior to LFR deployment.

**Table 8 — Demographic of subjects with high non-mated comparison scores in RFR testing**

| Non-mated comparison score                                                     | Female | Male | Asian | Black | White | Age <21 | Age 21-30 | Age 31-42 | Age >42 |
|--------------------------------------------------------------------------------|--------|------|-------|-------|-------|---------|-----------|-----------|---------|
| score $\geq 0.66$                                                              | 0      | 0    | 0     | 0     | 0     | 0       | 0         | 0         | 0       |
| score $\geq 0.64$                                                              | 1      | 0    | 0     | 1     | 0     | 0       | 1         | 0         | 0       |
| score $\geq 0.62$                                                              | 1      | 1    | 1     | 1     | 0     | 0       | 2         | 0         | 0       |
| score $\geq 0.60$                                                              | 1      | 3    | 2     | 2     | 0     | 1       | 3         | 0         | 0       |
| score $\geq 0.58$                                                              | 5      | 4    | 3     | 5     | 1     | 4       | 4         | 0         | 1       |
| score $\geq 0.56$                                                              | 11     | 6    | 4     | 11    | 2     | 5       | 9         | 2         | 1       |
| Identification searches:<br>gender, ethnicity & age balance                    | 51%    | 49%  | 28%   | 26%   | 46%   | 21%     | 28%       | 26%       | 25%     |
| <b>Notes:</b> Watchlist size:178,000; Non-mated identification searches: 3,943 |        |      |       |       |       |         |           |           |         |

Table 8 shows the demographics for high-scoring non-mated comparison scores arising from RFR testing, and we note that the demographic distribution is very similar to Table 6 showing the demographic distribution of LFR false positives. The majority of non-mated comparison scores at threshold 0.56 arose from probe images and recognition opportunities of subjects of Black ethnicity.

## 9.2 TPIR VARIATION IN PERFORMANCE & EQUITABILITY

In Section 8.4 demographic variation in performance was examined at the default face-match threshold of 0.6. At different thresholds the TPIR values can change for each demographic subgroup, and the statistically significant cases can vary.

## 9.3 FPIR EQUITABILITY

Equitability is dependent on the face-match threshold settings and on the size and demographic composition of the LFR watchlist or RFR reference database.

The demographic variation in the non-mated score distribution does not affect equitability if settings are such that the chance of a false alert is very low. However, if settings allow for a higher number of false alerts, these are likely to occur disproportionately within Black and Asian ethnicities.

## 9.4 EFFECT OF REFERENCE DATASET/WATCHLIST SIZE AND COMPOSITION ON FPIR

The size and composition of the watchlist tested in the study is useful for revealing demographic variation in performance of the algorithm, but equitability should be judged on a watchlist more typical of an operational deployment.

The candidates lists and comparison scores output by the batch RFR facial comparison program provide data to enable an estimation of FPIR of the Cohort probe dataset against subsets of the reference database of a specified size and demographic profile.

In identification systems configured to produce multiple candidates (such as RFR) Selectivity is the average number of candidates returned in a non-mated identification transaction where the comparison score exceeds the face-match threshold. Selectivity and FPIR differ at low thresholds but converge at high thresholds as false positives become rarer.

We can calculate Selectivity separately for each Gender-Ethnicity component of the Filler dataset:

$$\text{SEL}_{\text{FILLER}}(T) = \text{SEL}_{\text{Asian\_F}}(T) + \text{SEL}_{\text{Black\_F}}(T) + \text{SEL}_{\text{White\_F}}(T) + \text{SEL}_{\text{Asian\_M}}(T) + \text{SEL}_{\text{Black\_M}}(T) + \text{SEL}_{\text{White\_M}}(T)$$

and then scale each component in accordance with the specified size and demographic profile of the operational reference database, e. g., the scaling factor for  $\text{SEL}_{\text{Asian\_F}}(T)$  is:

$$\frac{\text{number of Asian Female reference images for operational watchlist}}{\text{number of Asian Female reference images in the Filler dataset}}$$

Summing the scaled components then calculates an average of number of candidates returned based on the specified demographic profile.

Applying this process to the RFR results for identification searches of Cohort Probes (of each demographic in turn) against the entire Filler dataset provides an estimate of the FPIR by demographic for the notional MPS watchlist (in Table 9) and SWP watchlist (in Table 10).

Note that when the observed selectivity is zero, or very low, the anticipated FPIR is given as '< 1 in 10,000' or '< 1 in 100,000': there are insufficient data points to support lower estimates.

**Table 9 – Selectivity and estimated FPIR by probe demographic for notional MPS Watchlist**

|                                                                                                                                                                                                                                                          | Asian Female             | Asian Male            | Black Female             | Black Male            | White Female             | White Male            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------------|--------------------------|-----------------------|--------------------------|-----------------------|
| Face match threshold: 0.66                                                                                                                                                                                                                               | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    |
| Face match threshold: 0.64                                                                                                                                                                                                                               | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    | 0.00003<br>< 1 in 10,000 | 0<br>< 1 in 10,000    | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    |
| Face match threshold: 0.62                                                                                                                                                                                                                               | 0<br>< 1 in 10,000       | 0.00011<br>1 in 9,200 | 0.00003<br>< 1 in 10,000 | 0<br>< 1 in 10,000    | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    |
| Face match threshold: 0.60                                                                                                                                                                                                                               | 0<br>< 1 in 10,000       | 0.00022<br>1 in 4,600 | 0.00021<br>1 in 4,700    | 0.00023<br>1 in 4300  | 0<br>< 1 in 10,000       | 0<br>< 1 in 10,000    |
| Face match threshold: 0.58                                                                                                                                                                                                                               | 0.00001<br>< 1 in 10,000 | 0.00033<br>1 in 3,000 | 0.00048<br>1 in 2,000    | 0.00046<br>1 in 2,100 | 0<br>< 1 in 10,000       | 0.00017<br>1 in 5,800 |
| Face match threshold: 0.56                                                                                                                                                                                                                               | 0.00008<br>< 1 in 10,000 | 0.00098<br>1 in 1,000 | 0.00109<br>1 in 920      | 0.00093<br>1 in 1,000 | 0.00004<br>< 1 in 10,000 | 0.00017<br>1 in 5,800 |
| <b>Notes:</b> <ul style="list-style-type: none"> <li>Notional MPS Watchlist: watchlist size 10,000 with demographic profile based on MPS arrest data</li> <li>In the table selectivity is shown as decimal, and estimated FPIR shown as ratio</li> </ul> |                          |                       |                          |                       |                          |                       |

In Table 9 we see that for the size 10,000 notional MPS watchlist at thresholds above 0.6 the extent of demographic variation in FPIR is quite limited. However, at threshold 0.56 the demographic variation observed for the full Filler dataset persists and, depending on numbers and demographic composition of the crowd, could show a noticeable effect on outcomes.

**Table 10 – Selectivity and estimated FPIR by probe demographic for notional SWP Watchlist**

|                                                                                                                                                                                                                                                     | Asian Female               | Asian Male                 | Black Female               | Black Male                 | White Female               | White Male              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|-------------------------|
| Face match threshold: 0.66                                                                                                                                                                                                                          | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000     |
| Face match threshold: 0.64                                                                                                                                                                                                                          | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0.000000<br>< 1 in 100,000 | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000     |
| Face match threshold: 0.62                                                                                                                                                                                                                          | 0<br>< 1 in 100,000        | 0.000002<br>< 1 in 100,000 | 0.000000<br>< 1 in 100,000 | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000     |
| Face match threshold: 0.60                                                                                                                                                                                                                          | 0<br>< 1 in 100,000        | 0.000003<br>< 1 in 100,000 | 0.000002<br>< 1 in 100,000 | 0.000003<br>< 1 in 100,000 | 0<br>< 1 in 100,000        | 0<br>< 1 in 100,000     |
| Face match threshold: 0.58                                                                                                                                                                                                                          | 0.000000<br>< 1 in 100,000 | 0.000005<br>< 1 in 100,000 | 0.000004<br>< 1 in 100,000 | 0.000006<br>< 1 in 100,000 | 0<br>< 1 in 100,000        | 0.000031<br>1 in 32,000 |
| Face match threshold: 0.56                                                                                                                                                                                                                          | 0.000012<br>1 in 86,000    | 0.000015<br>1 in 67000     | 0.000008<br>< 1 in 100,000 | 0.000012<br>1 in 84,000    | 0.000007<br>< 1 in 100,000 | 0.000031<br>1 in 32,000 |
| <b>Notes:</b> <ul style="list-style-type: none"> <li>Notional SWP Watchlist: watchlist size 1,000 with demographic profile based on SWP arrest data</li> <li>In table selectivity is shown as decimal, and estimated FPIR shown as ratio</li> </ul> |                            |                            |                            |                            |                            |                         |

Table 10 shows the demographic variation in performance changes for the demographic profile and size of the notional SWP watchlist. Moreover, even at face-match threshold 0.56, the FPIR is now below 1 in 30,000 for each ethnicity-gender, and the demographic variation is likely to be inconsequential unless the number of crowd subjects in the deployment is somewhat in excess of 32,000.

## 9.5 RETROSPECTIVE FACIAL RECOGNITION PERFORMANCE ON CHALLENGING FACIAL IMAGES

The perfect results from the testing of Retrospective Facial Recognition are very promising. It should be noted that all the face images were taken by test staff, or Cohort in the case of

selfies, and when a facial image taken considered unsatisfactory by the photographer, e.g., out of focus, motion blur, subject eyes shut, generally a second image would be taken. For evaluation of demographic equitability this was appropriate for the images need to be consistent across demographics. It should be acknowledged that using images of lower quality, or lower resolutions, may not achieve the same level of performance.

## 9.6 RECOGNITION AGAINST SAME-DAY IMAGE

Note that, in the evaluation, images were collected from Cohort subjects over one or two days. This is typical for such evaluations due to limitations on project duration, and the difficulty of obtaining a stable corpus of test subjects who can participate over an extended time-period. Other factors being equal, TPIR rates for facial recognition against a recent photograph are likely to be better than TPIR against historic photographs. In terms of demographic differentials in performance this means that the study has not been able to address the effects of 'template ageing'.

## 9.7 SUGGESTIONS FOR FURTHER INVESTIGATIONS

In the report we have made comment some issues where further information may be able to extend knowledge on how facial recognition systems perform in more challenging cases:

- effects of poor-quality video and video compression on Live Facial Recognition performance
- extending testing of Retrospective Facial Recognition to facial images of lower quality or resolution
- consideration of the effects of template ageing on performance and any demographic effects.

Policing may wish to consider how these issues relate to their use cases for RFR and LFR, and the nature of images they plan to use. Further controls or testing may be appropriate for facial images of lower quality or resolution. Some testing may be able to reuse the facial images and video collected for this study, downgrading the images in a controlled manner. The Filler dataset contained some cases where there were two or more time-separated facial images of data subjects. Such data might allow for assessment of demographic effects in template ageing.

## 9.8 TEST CORPUS ARISING FROM THE STUDY

The facial images and video footage collected in the study are to be provided to the Metropolitan Police Service along with associated ground truth metadata to enable reuse of the data for future testing of facial recognition systems.

## 10 TERMINOLOGY AND ABBREVIATIONS

**Candidate:** Image of a person from the watchlist or reference database returned as result of an identification search.

**Cohort:** Subjects recruited to provide a corpus of facial images and video for recognition in the evaluation.

**Comparison score:** Numerical value of the similarity between compared probe and reference facial images.

**Crowd:** Members of the public passing through the zone of recognition of the LFR system.

**Equitable:** Equitability of an operational deployment requires that differences, where any exist, in the outcomes for the subjects from different demographics should be inconsequential.

**Face-match threshold:** The comparison score value above which the compared images will be considered to match.

**FPIR: False Positive Identification Rate** (for LFR) is the proportion of recognition opportunities of subjects who are not on the watchlist which return a (false positive) match against a candidate on the watchlist.

$$\text{FPIR}(N, T) = \frac{\text{Num. non-mated recognition opportunities that return a match against a candidate on the watchlist}}{\text{Num. non-mated recognition opportunities}}$$

where  $N$  represents the number of images on the watchlist, and  $T$  the face-match threshold.

**Filler dataset:** Dataset drawn from MPS holdings of custody images and used to supplement Cohort reference images to provide large reference dataset for the evaluation.

**LFR:** Live Facial Recognition

**Mated:** A mated identification search is one in which the subject in probe image also has a reference image in the reference database. A mated recognition opportunity is one where the subject walking through the LFR zone of recognition has an image in the LFR watchlist. Similarly, a mated comparison score is produced from comparisons of two face images of the same individual.

**Non-mated:** A non-mated identification search is one in which the subject in probe image does not have a reference image in the reference database. A non-mated recognition opportunity is one where the subject walking through the LFR zone of recognition does not have a facial image in the LFR watchlist. Similarly, a non-mated comparison score is produced from comparison of face images of different individuals.

**MPS:** Metropolitan Police Service

**NEC:** NEC Software Solutions – the company providing the Neoface facial recognition technology evaluated in this report

**OIFR:** Operator Initiated Facial Recognition

**Probe image:** A facial image that is searched against a watchlist or reference database.



**Rank:** The rank of a candidate facial image is its position in the set of candidates returned by an identification search listed in decreasing order of similarity to the probe (i.e., the Rank-1 candidate is the best matching candidate).

**Reference image:** A facial image in the watchlist or reference database.

**Recognition opportunity:** The period when a subject moves through the zone of recognition of an LFR system with their face visible to the LFR camera.

**RFR:** Retrospective Facial Recognition

**SEL: Selectivity** (for RFR) the average number of candidates returned in a non-mated identification transaction for which the candidate comparison score exceeds the face-match threshold.

$$SEL(N, T) = \frac{\text{Total Num. candidates returned with score above threshold } T \text{ in the set of non-mated identification transactions}}{\text{Num. non-mated identification transactions}}$$

where  $N$  represents the number of images on the watchlist, and  $T$  the face-match threshold.

**SWP:** South Wales Police

**TPIR: True Positive Identification Rate** (for LFR): the proportion of mated recognition opportunities that are correctly identified.

$$TPIR(N, 1, T) = \frac{\text{Num. mated recognition opportunities correctly identified}}{\text{Num. mated recognition opportunities}}$$

where  $N$  represents the number of images on the watchlist, and  $T$  the face-match threshold (the '1' denotes that LFR only considers the top match.) In policing this is often referred to as the True Recognition Rate.

**TPIR: True Positive Identification Rate** (for RFR & OIFR) is the proportion of mated identification searches that include the mated reference among the candidates returned.

$$TPIR(N, R, T) = \frac{\text{Num. mated identification searches where the mated reference is among the candidates returned}}{\text{Num. mated recognition opportunities}}$$

where  $N$  represents the number of images on the watchlist,  $R$  the number of best matching candidates returned and  $T$  the face-match threshold ( $T=0$  if no threshold is applied).

**Watchlist:** A set of reference images (of individuals of interest to policing) against which a probe image is searched.

**Zone of recognition:** Three-dimensional space within the field of view of the Live Facial Recognition camera and in which the imaging conditions for robust facial recognition are met.

## BIBLIOGRAPHY

- [1] 'Facial Recognition Technology in Law Enforcement Equitability Study - Test Strategy', 2022, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/other-lfr-documents/equitability-study-test-strategy.pdf>
- [2] ISO/IEC 19795-1:2021 Biometric testing and reporting - Part 1: Principles and framework
- [3] ISO/IEC 19795-2: 2007 Biometric testing and reporting - Part 2: Testing methodologies for technology and scenario evaluation
- [4] NPL & MPS, 'Metropolitan Police Service Live Facial Recognition Trials 2016-2019', February 2020, <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf>
- [5] Office for National Statistics, 'Ethnic group, England and Wales: Census 2021', <https://www.ons.gov.uk/peoplepopulationandcommunity/culturalidentity/ethnicity/bulletins/ethnicgroupenglandandwales/census2021>
- [6] Gov.uk, 'Arrest Data March 2018 to March 2021', <https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest/downloads/arrests-data-march-2018-to-march-2021.csv>
- [7] NPIA, 'Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images', National Policing Improvement Agency, 2007
- [8] ISO/IEC 30137-1:2019 Use of biometrics in video surveillance systems - Part 1: System design and specification
- [9] N. Yager and T. Dunstone, 'The Biometric Menagerie', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 2, pp. 220-230, 2010

## ACKNOWLEDGEMENTS

The work was funded by the Home Office with Science, Technology, Analysis & Research (STAR) funding through the Metropolitan Police Service. (MPS)

MPS support to the project included:

- Provision of server and Neoface Facial Recognition software licence,
- Provision of camera and mobile devices for photographing various types of facial images including taking custody style images consistent with those in operational policing,
- Providing a demographically balanced 'filler dataset' of custody images to serve as a large watchlist for the evaluation,
- Volunteer police cadets to provide test subjects between ages 12 and 18,
- Running of operational LFR deployments to collect video footage of our test Cohort in operational conditions,
- Obtaining a venue in the vicinity of the LFR deployment for NPL to brief and photograph the test Cohort.

South Wales Police support to the project included:

- Running of an operational LFR deployments to collect video footage of our test Cohort in operational conditions,
- Providing a venue in the vicinity of the LFR deployment for NPL to brief and photograph the test Cohort.

Ingenium Biometrics assisted NPL in the taking still photographs and video footage of the test Cohort alongside the Policing LFR deployments.

Ingenium Biometrics and The School of Engineering, University of Kent assisted in providing technical review of the evaluation, analyses, results, and report.

# MPS Live Facial Recognition

## 1. Policing Need & Intel Case

### MPS LFR summary process for a stand-alone deployment

#### Key MPS LFR Document References

Applicant identifies a policing need which LFR has the potential capability to meet in line with the MPS Objectives for LFR use and Met Direction.

- Policy: Section 5.
- Legal Mandate: Section 2

Intelligence case commissioned in relation to the policing need – the intelligence case will inform the LFR planning process and ensure the use of LFR is intelligence-driven.

- Policy: Section 6.1
- SOP: Section 5 and .6
- MPS LFR Form 3: Intelligence Case

Applicant to apply to AO for approval to Deploy

- MPS LFR Form 1, Part 1: Application

**1** Location, date, time, rationale to be defined. If the location raises higher expectations of privacy this is to be explained and any additional safeguards / mitigations outlined

**2** Legal basis and legitimate aim to be defined. Applicant to explain how the Deployment will achieve the legitimate aim(s) informed by the intelligence case.

**3** ECHR Articles engaged to be specified. This will include Art. 8 and may include 9, 10, 11 & 14.  
- Data protection grounds (Schedule 8) for sensitive processing to be identified.

**4** Necessity case articulated – why is it necessary to achieve the legitimate aim in a democratic society and why is the processing of data is strictly necessary?  
- Pressing social need to be identified

- SOP: Section 5.
- Legal Mandate: Section 3.8 and 3.10 – 3.12

- Legal Mandate: Sections 1.1 – 3.9
- Policy: Section 5

- Legal Mandate: Sections 3 and 5
- DPIA

**5** Proportionality case to be articulated. To include the importance of the objective, alternatives, public awareness steps and other deployment-specific measures to ensure the least possible intrusion.

**6** Watchlist composition to be proposed and how its construction is supported by the intelligence case explained. The necessity and proportionality for the Watchlist composition is to be detailed.

**7** Watchlist composition regarding under 13 and 18, the disabled, gender transition and any use of non-police originated images to be detailed, supported by a rationale for AO's consideration.

**8** Compliance with the MPS LFR Documents to be confirmed / explained for the AO's consideration. DPIA, EIA, CIA, any supporting legal advice and technical advice to be submitted to AO

- Legal Mandate: Section 3
- Policy: Section 4.10
- SOP: Section 5

- Legal Mandate: Section 3
- Policy: Sections 5.5, 10.3 to 10.8
- SOP: Section 6

- Legal Mandate: Section 3
- Policy: Sections 4 - 6
- SOP: Section 6

AO to consider the LFR application to Deploy

- MPS LFR Form 1, Part 2: Written Authority Document
- Policy: Section 4 regarding Urgency

AO to consider the LFR Application and confirm if they authorise it, reject it, or require further amendments. The AO's role will include recording a decision for LFR Document compliance, (ii) Legitimate Aim, (iii) Human Rights – Necessity, (iv) Data Protection – Necessity, (v) Proportionality, (vi) Watchlist Composition, and (vii) Deployment location and times.

The AO will provide a high degree of scrutiny to any proposals for Watchlists which include those under 13 or 18, the disabled, gender transition or the inclusion of non-police originated images and any proposal to deploy which raises elevated privacy concerns.

AO to review and adopt (amending where necessary and appropriate) the DPIA, EIA, the SCC Self-Assessment.

AO to review the Community impact Assessment particularly in the context of Watchlist composition and those likely to pass the LFR system.

AO to engage with SRO, DPO, DLS, CPIE Engagement Team and Technical as necessary to seek advice to inform their decisions. .

AO to direct Police Officers and Staff engaged in the Deployment to receive MPS LFR Training.

- An AO must be very familiar with the MPs LFR Documents in order to provide a high degree of scrutiny when considering an LFR application.
- The AO may be guided to particularly relevant sections of the MPS LFR documents by reference to those highlighted above for the MPS LFR application.

AO to engage with an officer of NPCC rank to ensure strategic issues from a pan-London perspective are considered

- Policy: Section 7.5

AO grants authority to deploy LFR.  
AO to confirm the LFR Gold for the Deployment. The Gold appoints the remainder of the Deployment command structure.

- Policy: Sections 5.1, 7.3 – 7.6
- SOP: Sections 4, 10.1 – 10.2

## 2. Application To Deploy LFR Made

## 3. Written Authority Document

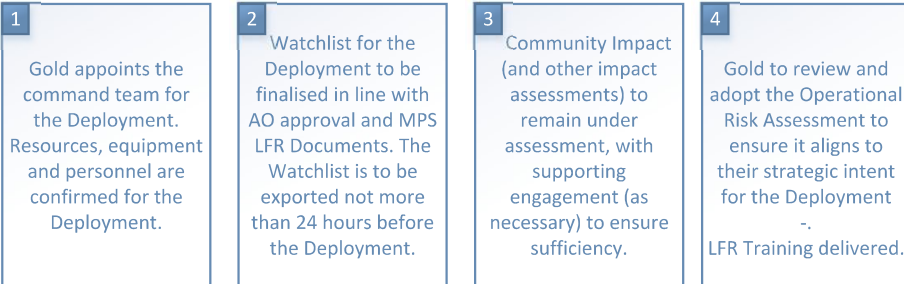
# MPS Live Facial Recognition ... cont.

## 4. Pre-Deployment Activity

### MPS LFR summary process for a stand-alone deployment

#### Key MPS LFR Document References

Pre-Deployment activity undertaken under the direction of Gold to implement the AO's authority to Deploy.



- Policy: Section 7
- SOP: Sections 7 - 10

1

- Policy: Section 10
- SOP: Section 6

2

- Policy: Section 7
- SOP: Sections 7 and 10

3

4

## 5. LFR Deployment

Public engagement measures implemented to support the overt use of LFR to locate persons on a Watchlist and to support data subjects being aware of their individual rights.

- Policy: Section 9
- SOP: Sections 5.7 -5.8

Watchlist imported into LFR system. LFR Cameras established, roles confirmed and personnel deployed.

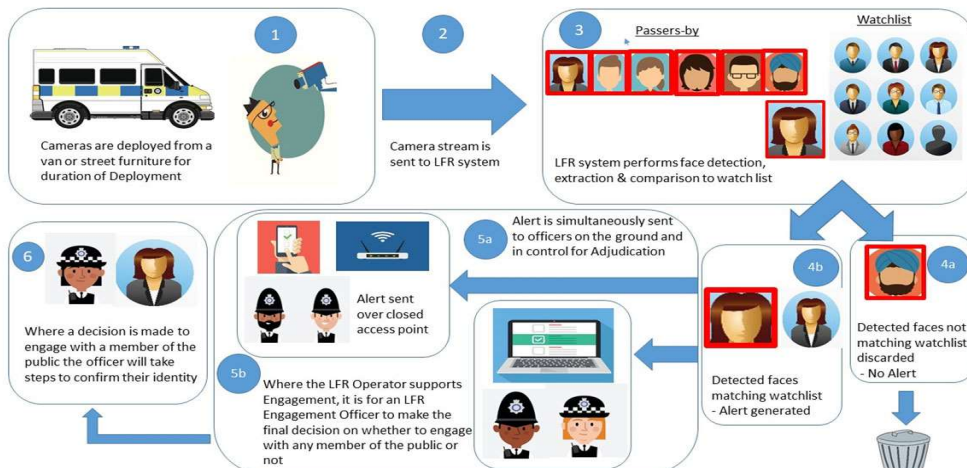
- Policy: Sections 10 and 12
- SOP: Section 6 and 10

LFR Deployment undertaken. The Deployment is to remain under review in line with the AO's authority, the MPS LFR Documents and the assessments which support the Deployment. Key metrics are to be recorded to support the ongoing assessment of LFR performance and to aid transparency with the public post-Deployment.

Those responsible for the Deployment need to have familiarity with the MPS LFR Documents.

- Policy: Sections 7, 9.5 and 13
- SOP: Sections 10 and 11.3

A summary of how the LFR process works in relation to an individual passing the LFR system



## 6. Post-Deployment Activity

Gold to ensure a post-Deployment evaluation is completed with a Cancellation Report being produced. This supports the capture of learning for future deployments and helps inform activity to ensure ongoing measures to assure the performance of the algorithm.

- MPS LFR Form 1, Part 3: Cancellation Report
- Policy: Sections 7, 10.9 – 10.14 and 11

Data only to be retained where it is necessary to do so and it should be retained and managed in line with MPS LFR Documents.

- Policy: Section 7
- SOP: Section 13
- Legal Mandate: Section 5
- DPIA

Register of Deployments to be updated and published.

- Policy: Section 9.6
- SOP: Section 13

## FACIAL RECOGNITION OVERVIEW

|                              |                            |                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                           |
|------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Types of Facial Recognition: |                            | The use of facial recognition where all persons passing the system’s camera(s) are analysed by the system with results being generated in tandem with events.                                                                                                                  | The use of facial recognition where:<br>(i) media is directly captured of a subject present; or<br>(ii) media is otherwise acquired in lieu of capturing it, with the intent of subjecting it to analysis by the facial recognition system. The results of such analysis could shape events to which the footage relates in real time. | The use of facial recognition where media is analysed after the event. The result of such analysis would come sufficiently after the event such that they could not shape events to which the media related in real time. |
| Overt                        | Name                       | Live Facial Recognition (LFR)                                                                                                                                                                                                                                                  | Operator Initiated Facial Recognition (OIFR)                                                                                                                                                                                                                                                                                           | Retrospective Facial Recognition (RFR)                                                                                                                                                                                    |
|                              | How it may be referred to: | “... the use of overt live facial recognition to locate people on a watch list who are sought by the police ...”                                                                                                                                                               | “... the use of operator initiated facial recognition which takes an image of a particular person and uses it to either (i) help policing establish who a person in the image is or (ii) establish where a person has previously appeared in other media held by the police ...”                                                       | “... retrospective facial recognition may be used after an event to help officers establish who a person is or whether their image matches against other media held on databases ... “                                    |
| Covert                       | Name                       | Covert Real-Time Facial Recognition Surveillance (CRFRS)                                                                                                                                                                                                                       | Covert Operator Initiated Facial Recognition Surveillance (COIFRS)                                                                                                                                                                                                                                                                     | RFR is not a covert capability in itself. It may however use media obtained via covert means.                                                                                                                             |
|                              | How it may be referred to: | ... “whilst the then Surveillance Camera Commissioner has recognised a possible application for facial recognition in a covert way, subject to the Regulation of Investigatory Powers Act 2000, policing does not comment on any potential use of covert policing tactics ...” |                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                           |



More Trust | Less Crime | High Standards

|                          |                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------|
| Classification           | Official                                                                                             |
| Suitable for Publication | Yes                                                                                                  |
| Title                    | Appropriate Policy Document for sensitive data processing within Live Facial Recognition deployments |
| Purpose                  | Policy to outline the MPS's governance and compliance against Section 42 Data Protection Act 2018    |
| Author                   | MPS LFR                                                                                              |
| Version                  | 2.0                                                                                                  |
| Creating Unit            | MPS LFR                                                                                              |
| Date Created             | 20 <sup>th</sup> March 2023                                                                          |
| Review Date              | 20 <sup>th</sup> March 2024                                                                          |

## MPS Appropriate Policy Document: Live Facial Recognition

**Terms & Definitions:** Capitalised terms used in this MPS LFR Appropriate Policy Document shall have the meaning given to them in the MPS LFR Policy Document unless otherwise defined in this MPS Appropriate Policy Document: Live Facial Recognition.

---

Part 3 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement (LE) purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to GDPR special category data. This includes:

- a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- c) the processing of data concerning health;
- d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. Given Live Facial Recognition involves the processing of biometric data, section 35(5) requires this processing to be lawful and fair. The processing is only to occur

where it is strictly necessary for the LE purpose and is based on a Schedule 8 condition. The MPS LFR Documents explain how this is achieved.

This document and the wider MPS LFR Documents together demonstrate that the MPS's processing of sensitive data in respect of live facial recognition technology (LFR) is compliant with the requirements with Part 3, Section 42 of the DPA 2018. In compliance with Section 42(2) of the DPA 2018 it explains the procedures and measures for securing compliance with the LE data protection principles and explains the policies as regards retention and erasure of personal data.

This document should be treated as being complimentary to the MPS general record of processing under S61 DPA 2018 and the MPS LFR Documents. It also complements the MPS' policy on protecting special category and criminal convictions policy.

### **Description of data processed - the data created by the LFR system**

Biometric data: LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify possible matches against persons of interest to LEAs. Where the LFR system identifies a potential image match, the LFR system flags an Alert to a trained member of MPS personnel who then makes a decision as to whether any further action is required. The LFR system therefore creates biometric data in two ways:

- the Templating of images of those included on a Watchlist produces personal biometric data; *and*
- the Templating of facial images from passers-by also produces personal biometric data for each face detected by the LFR cameras.

Other Personal Data: The use of LFR technology involves the creation of personal data. This includes the CCTV feed from the LFR system. It also includes metadata such as the time and location that people pass through the LFR system. Personal data (such as a person's name) may also be obtained as part of the Engagement process.

### **Description of data processed - the data used by the LFR system**

A bespoke Watchlist is imported into the LFR system for each Deployment. As well as including images of those being sought, it includes their name, date of birth, the date and location where the image was taken and the reason why they are of interest to the MPS. This data is handled in accordance with MOPI, in line with the MPS's wider policies on managing police data.

The data is typically drawn from the electronic warrants management system (EWMS), MPS custody and PNC. Data may be provided by other police forces and agencies associated with law enforcement as well as the wider public as they would more generally to assist the MPS with its law enforcement duties. This would be particularly relevant in relation to missing persons where the image and other data may be provided by that person's family.

### **Level, frequency of data being processed and the individuals impacted**

The below table summarises the key points during an LFR Deployment and the level, frequency, and nature of the data being processed. It also identifies those whose data is processed.



| <b><u>Level of data being processed</u></b>                 | <b>Those on a Watchlist</b>                                                                       | <b>Those Engaged as a result of an Alert</b>                                                   | <b>Everyone who passes the LFR system</b>                         |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>Biometric Processing</b>                                 | <b>Yes</b>                                                                                        | <b>Yes</b>                                                                                     | <b>Yes</b>                                                        |
|                                                             | Biometric Templates are created for those on a Watchlist.                                         | Biometric Templates are created for those passing the LFR system.                              | Biometric Templates are created for those passing the LFR system. |
| <b>Imagery</b>                                              | <b>Yes</b>                                                                                        | <b>Yes</b>                                                                                     | <b>Yes</b>                                                        |
|                                                             | The image uploaded to the Watchlist is available to officers following an Alert.                  | An image of the individual passing the LFR system is available to officers following an Alert. | The CCTV feed from the LFR deployment is recorded.                |
| <b>Criminal convictions data</b>                            | <b>Yes</b>                                                                                        | <b>Yes</b>                                                                                     | <b>No</b>                                                         |
|                                                             | The reason why a person is being sought by the MPS is available to an officer following an Alert. | Personal data may be obtained - based on a policing need to verify an Alert.                   |                                                                   |
| <b>Personal data (such as name, date of birth, address)</b> | <b>Yes</b>                                                                                        | <b>Yes</b>                                                                                     | <b>No</b>                                                         |
|                                                             | The details of the person being sought by the MPS is available to an officer following an Alert.  | Personal data may be obtained - based on a policing need to verify an Alert.                   |                                                                   |
| <b>Metadata</b>                                             | <b>Yes</b>                                                                                        | <b>Yes</b>                                                                                     | <b>Yes</b>                                                        |
|                                                             | In relation to the images uploaded to the Watchlist.                                              | In relation to those passing the LFR system.                                                   | In relation to those passing the LFR system.                      |

Data is processed in relation to a specific LFR Deployment, the frequency of LFR Deployments being based on the intelligence case causing it to be necessary and proportionate to use LFR in furtherance of the MPS's common law policing powers and the availability of resource.

The number of people on a Watchlist will vary between Deployments. Rather than being driven by the LFR system's capacity, the inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality. The number of people on a Watchlist will therefore need to be as small as possible, whilst still achieving a legitimate policing purpose.

The number of people passing an LFR system will also vary between Deployments. Factors such as the time of day, Deployment length, nearby facilities, infrastructure, and public events will all influence the footfall expected to pass an LFR system. The MPS LFR SOP outlines the criteria for images that may be considered appropriate for use on a Watchlist. The MPS LFR SOP also outlines considerations as to the source of an image that may be used on a Watchlist, noting that some imagery may engage greater privacy expectations than others. These controls assist the public and decision-making officers to understand LFR and how it may be used.

## Geographical scope

LFR will be used for a limited time, with a limited footprint, with a limited purpose of seeking to locate those whose presence is of justifiable interest to the MPS. Whilst LFR may be used at locations across London, any Deployment will be limited to a specific location using hardwired cameras linked to the LFR system. The locations used will be based on the intelligence case to Deploy LFR, the requirements of the LFR system and considerations relating to privacy that may attach to a particular area (as more particularly outlined in the MPS LFR Legal Mandate and the MPS LFR SOP).

## Data storage and review

Data storage on the LFR system: The LFR system is a fully closed system with two layers of password protection to access the application. The LFR system is physically protected when in use and securely wiped following each Deployment. Access to the LFR system is limited to those with a need to use it.

Importing onto the LFR system: Images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine. Access to the USB stick containing the Watchlist is limited to those with a need to use it.

Data storage on wider MPS systems: The data is held securely on MPS systems accessible via the MPS computer system, Aware. Officers leaving the MPS automatically have their account disabled and therefore would no longer have access to the information. The data held on the MPS systems is not specific to LFR (it provides LFR with the information needed to compile and generate a Watchlist and relates to policing information generated following LFR Alerts). The MPS has its own policy on retention, review and disposal that applies to this information, including the need to hold and review policing information in accordance with MOPI and CPIA (as applicable).

## Data retention

With regards to data retention, the MPS LFR Documents provide that:

- where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*
- the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:

- personal data is retained in accordance with the DPA 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
- personal data is retained beyond the 31 day period in accordance with the MPS's complaints / conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

- in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
- in accordance with the MPS's complaints / conduct investigation policies; *and/or*
- in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

### **The right to request data erasure**

The right to erasure allows data subject to request erasure of their personal information. This enables data subjects to ask the MPS to delete or remove personal information where there is no lawful reason for the MPS to continue to process it. This right is not specific to LFR but applicable to all personal data processed by the MPS. LFR therefore does not restrict this right – in fact, the data created by LFR which no longer needs to be retained is deleted by default. This includes:

- where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; and
- the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable and in any case, within 24 hours following the conclusion of the Deployment.

Right to restriction enables the data subject to ask the MPS to suspend the processing of personal information about the data subject, for example if they want the MPS to establish its accuracy or the reason for processing it. This right is not specific to LFR but applicable to all personal data processed by the MPS with established processes in places to facilitate such requests.

Additionally to uphold the right to erasure and restriction, the MPS has taken a number of further measures including:

- MPS Privacy Notice: This provides that requests for data erasure or restriction may be provided to the Information Rights Unit at: [SARenquiries@met.police.uk](mailto:SARenquiries@met.police.uk) or via post to MPS Information Rights Unit, PO Box 313, Sidcup, DA15 0HH.
- MPS website: This provides the public with a copy of the MPS Privacy Notice that details how the right to erasure or restriction may be exercised.
- MPS policy: and guidance is provided by the MPS's Information Rights Unit to ensure the MPS complies with this legal obligation.

### **Watchlist data**

The LFR Operator has the ability to delete images from the Watchlist and will record such action in their log. This may be necessary when a valid request for erasure is received. It may also be necessary if a person was validly placed on a Watchlist at the point the Watchlist was imported into the LFR system but was subsequently located by LFR and dealt with by the MPS before passing the same LFR Deployment later in the day. In these circumstances and to mitigate against future Alerts being generated, the image may be removed by the Operator from the Watchlist.

## **Data sharing**

Should the LFR system generate an Alert, the subsequent process would typically also involve MPS personnel using policing databases and other intelligence systems to inform any further action. This subsequent action may also involve the MPS working with other police forces, law enforcement bodies and other agencies to assist the MPS in discharging its common law policing powers. This action will not require the sharing of biometric data but may require the MPS to share personal data, as it would for any investigation, in accordance with the MPS's routine sharing arrangements.

## **Consent or Schedule 8 condition for processing**

It is not practical to obtain consent of all data subjects whose data is processed in relation to the use of LFR. The MPS relies on there being a strict necessity to process the data for its LE purposes. The MPS also relies on Schedule 8. Whilst the Authorising Officer will confirm the Schedule 8 ground being relied on as part of the authorisation process, this will typically be that the Deployment of LFR is necessary for judicial and statutory purposes – for reasons of substantial public interest. This is further explained in the MPS LFR Documents, particularly the MPS LFR Legal Mandate.

## **The Accountability principles**

The MPS has in place appropriate technical and organisational measures to meet the requirements of the accountability principle. These include:

- data protection policies and other documentation which in the context of LFR include the MPS LFR Legal Mandate, the MPS LFR DPIA, the MPS Privacy Notice, the MPS' policy on protecting special category and criminal convictions policy and the other MPS LFR Documents;
- detailed security measures relating to the LFR system;
- a 'data protection by design and default' approach to the LFR system which includes the deletion of the biometric data of those who are Templated by the LFR system on entering the Zone of Recognition but do not trigger an Alert;
- maintaining logs in relation to the LFR system in relation to decision making and Alerts – as further detailed in the MPS LFR SOP;
- data protection measures and policies to record and, where necessary, report personal data breaches;
- the appointment of a data protection officer;
- responding to guidance and documentation produced by the Surveillance Camera Commissioner, the Biometrics Commissioner and the Information Commissioner; *and*
- a process for ongoing review, both post-Deployment and in relation to the MPS LFR Documents. The Data Protection Officer (DPO) also has oversight of this via the MPS LFR Strategic Board.

## **Principle 1: Lawfulness and fairness**

The lawfulness of the MPS's use of LFR: The MPS LFR Legal Mandate outlines:

- the legal basis on which LFR may be used by the MPS;
- the grounds when LFR may be used on the basis that it is strictly necessary for a LE purpose;
- confirmation that a condition of schedule 8 will be met;
- the safeguards and mitigations relating to data processing, human rights considerations; and
- how the MPS upholds the Public Sector Equality Duty.

The MPS LFR SOP and the MPS LFR Legal Mandate in particular provides detailed guidance to Authorising Officers on their responsibilities when considering if the Deployment of an LFR system is lawful and strictly necessary. This includes consideration of (i) what other policing methods have been used / discounted prior to using LFR, (ii) the importance of achieving the LE purpose and the prospective of achieving it through the use of LFR (iii) the size and scale of the proposed LFR Deployment and (iv) if the LE purpose which would underpin the use of LFR is strictly necessary and proportionate (not just desirable) to the need to undertake special category data processing and the risk to individual's rights.

The fairness of the MPS's use of LFR: The MPS Legal Mandate and the other MPS LFR Documents also explains how the MPS processes data fairly. Fairness is particularly relevant in two respects:

- Accessibility and foreseeability: The MPS LFR Documents are a control that regulates the discretion the police have to use facial recognition technology under its common law powers. By publishing these documents online, they are available to the public in a way that is accessible to them. Together with the MPS's commitment to give prior notification of its Deployments, the documents also allow the MPS's use of LFR to be foreseeable to the public. The objective here is that the public should be able to read the documents and understand them. It should allow the public to anticipate how the MPS will use LFR and the policing need LFR allows the MPS to address. For example the Watchlist image criteria in the MPS LFR SOP allows the public to understand the circumstances when an image may be considered for inclusion on a Watchlist.
- Fairness 'by design': The MPS has published a paper entitled 'Understanding the Metropolitan Police Service LFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its LFR algorithm.

Additionally, in relation to fairness, the MPS has also taken the following measures:

- Ongoing reviews to mitigate risks of unfairness: Informed by its Equality Impact Assessment, the MPS LFR Documents already provide for ongoing evaluation and a post-deployment review process for LFR Deployments on a per Deployment basis. This also offers the MPS a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS's Facial Recognition Strategic Board which reviews the performance of the LFR system at a strategic level.
- Training to ensure fairness: The MPS LFR Documents provide that officers and staff involved with an LFR Deployment will receive training. This is beneficial to ensuring fairness, particularly during the Adjudication Process. During this process, when an officer is deciding whether to Engage a member of the public, police officers are required to exercise their own judgement based on their training and experience. The training includes ensuring officers understand the characteristics of the LFR system that could affect the likelihood that an Alert is reliable – this specific training has a number of purposes including helping guard against the assumption that because an Alert has been generated it may be assumed to be correct. Police officers and staff also receive training to on discrimination and bring this knowledge to bear when discharging their duties.

Making available appropriate privacy information: The MPS has a mature Information Governance Strategy and Structure in place. It incorporates the requirements of the MPS to be open and transparent (wherever appropriate and possible) about how data is processed. To this end, and

having considered the risks to this right posed by the use of LFR, the MPS has adopted a number of measures to ensure that the right to be informed is upheld. The MPS LFR Documents provide details about how:

- the LFR system will be used overtly; and
- the MPS will ensure the public are aware regarding how their personal data is processed in relation to LFR.

This includes the use of prominent signage, leaflets and officers assisting the public during a Deployment. It will also include the use of the MPS's online channels to make the public aware of the use and results on LFR.

A key measure is the publication of the MPS Privacy Notice, the MPS policy on protecting special category and criminal convictions, and key MPS LFR Documents on the MPS website. Whilst the MPS is not required to publish a number of these documents, it has elected to do so. This is an important measure to inform Londoners including the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the Metropolitan Police Service (MPS), as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist. In this way, the MPS's use of LFR is both foreseeable and assessable. The published documents provide information as set out in the table below.

| <b>Key documents available to the public</b>                              | <b>Information included</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MPS Privacy Notice:</b>                                                | <ul style="list-style-type: none"> <li>• Data Controller identity and contact details</li> <li>• Data Protection Officer details</li> <li>• The scope and purposes for processing personal data by the MPS</li> <li>• Data retention periods</li> <li>• Data sharing arrangements</li> <li>• Data security</li> <li>• Rights as a data subject (including access, rectification and erasure)</li> <li>• Complaints (including the right to make a complaint to the ICO and contact details).</li> </ul> |
| <b>MPS policy on protecting special category and criminal convictions</b> | <ul style="list-style-type: none"> <li>• The MPS approach in relation to protecting and processing special category and criminal convictions data in relation to the data protection principles</li> <li>• The responsibilities of the Data Controller</li> <li>• Information relating to erasure and retention</li> <li>• How further information may be sought.</li> </ul>                                                                                                                            |
| <b>MPS LFR Legal Mandate</b>                                              | <ul style="list-style-type: none"> <li>• The lawful basis for processing data in relation to LFR. Including in relation to: <ul style="list-style-type: none"> <li>○ Common law policing powers</li> <li>○ Human Rights Act 1998</li> <li>○ Equality Act 2010</li> <li>○ Protection of Freedoms Act 2012</li> <li>○ Data Protection Act 2018</li> <li>○ Freedom of Information Act 2000</li> </ul> </li> </ul>                                                                                          |

| Key documents available to the public                                                               | Information included                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MPS Policy Document</b>                                                                          | <ul style="list-style-type: none"> <li>• An outline, strategic intent and objectives for the use of LFR and how personal data will be used by the LFR system</li> <li>• Key terms used across the MPS LFR Documents</li> <li>• Data retention periods applicable to LFR</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>MPS LFR Standard Operating Procedure Processes</b>                                               | <ul style="list-style-type: none"> <li>• Outlines measures relevant to considering where LFR can be Deployed by the MPS.</li> <li>• Watchlist considerations including the basis on which images may be added to a Watchlist and considerations relevant to the sources of non-police originated imagery.</li> <li>• Provides that during any policing operation where LFR is Deployed officers will be available to assist member of the public with queries, and: <ul style="list-style-type: none"> <li>○ signs publicising the use of the technology must be prominently placed in advance (outside) of the Zone of Recognition; and</li> <li>○ any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology.</li> </ul> </li> <li>• Both of these measures will be easy to read and together will ensure those passing the LFR system/who are Engaged by it will have the opportunity to seek further information. Both the signs and leaflets will provide an accessible QR code and website link to the MPS website for more information.</li> </ul> |
| <b>MPS LFR DPIA</b>                                                                                 | <ul style="list-style-type: none"> <li>• Describes the nature, scope, context and purposes of the processing.</li> <li>• Assesses necessity, proportionality and compliance measures.</li> <li>• Identifies and assesses risk to individuals.</li> <li>• Identifies any additional measures to mitigate those risks.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>MPS LFR Appropriate Policy Document</b>                                                          | <ul style="list-style-type: none"> <li>• Explains how the processing of sensitive personal data is compliant with the requirements of Part 3, section 42 of the DPA 2018.</li> <li>• Explains how the MPS complies with the Law Enforcement data protection principles. Outlines policies as regards the retention and erasures of personal data.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b><u>Understanding The Metropolitan Police Service LFR System's Accuracy and Bias Position</u></b> | <ul style="list-style-type: none"> <li>• Explains in a public-facing summary: <ul style="list-style-type: none"> <li>○ how to understand LFR system accuracy;</li> <li>○ what the MPS have done to understand its algorithm within an operational context.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b><u>MPS LFR EIA</u></b>                                                                           | <ul style="list-style-type: none"> <li>• Explains the MPS's approach to its responsibilities in relation to the Public Sector Equality Duty.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## **Principle 2: Purpose limitation**

Personal information must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes.

As the use of LFR is an operational one, the AO is required to be satisfied with the legitimate aim and the legal basis for the Deployment. Key considerations relating to necessity and proportionality are addressed in depth as part of the authorisation process.

The MPS LFR Legal Mandate also outlines MPS law enforcement purposes that can lawfully apply to justify the use of LFR. The law enforcement purpose for each Deployment will be articulated and authorised by the AO within the Written Authority Document. The MPS LFR Documents provide a structure to ensure that data is only processed for the authorised law enforcement purpose.

Should a further law enforcement purpose be identified after the AO has authorised an LFR Deployment, processing in respect of the further law enforcement purpose is not permissible unless the AO provides an authority that covers the further law enforcement purpose. Such authority would consider the lawfulness, strict necessity and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.

LFR Deployments will be subject to regular review to ensure that the LFR system and its operation remains necessary, proportionate and effective in meeting its use case.

## **Principle 3: Data minimisation**

The MPS LFR Documents provide that the MPS will only process data that is relevant and proportionate to its law enforcement policing purposes. There are a number of systems and processes in place to ensure this. These are set out below.

### Application & Authorisation

The LFR Application process adopted by the MPS requires applicants to consider and demonstrate necessity in considerable detail. Once this and other stages are satisfactorily completed, the Application then progresses into the Authorisation phase, where a senior MPS police officer (the Authorising Officer) considers necessity as part of any authority they provide for the use of LFR.

The AO needs to be satisfied that the Deployment is necessary to the standards required by the Human Rights Act 1998 and Data Protection Act 2018 in relation to biometric processing. This process makes clear that the need to use LFR should not be merely desirable, but is needed to meet a law enforcement purpose. This process also provides that any proposed processing that does not satisfy the necessity threshold should be challenged and not authorised.

By way of example, the AO must be satisfied by the steps taken to ensure that composition of a Watchlist is not excessive, and only includes those who need to be located by the MPS using LFR, on a strict necessity basis.

### Ongoing Review

The MPS LFR Documents require that on an ongoing basis, the Gold and Silver Commanders review the Deployment to ensure that it continues to meet the strict necessity threshold, and the requirements of proportionality. The Gold and Silver Commanders are obligated to stop the Deployment at any point, should the Deployment fail to meet the requirements of this Data



Protection Principle (amongst other reasons). The LFR Operator is also required to ensure that the LFR system is correctly working and will advise the Silver Commander should they identify any issues.

### **Relevance**

There are a number of requirements that help to ensure the Deployment is relevant to its legitimate aim and to ensure the relevance of the data being processed. These include:-

1. the need for a Deployments, and the location of the Deployment to be supported by intelligence and other policing information to confirm the need for the Deployment and the prospects for locating those sought;
2. the inclusion of an individual(s) on a Watchlist is to be:
  - a. supported by intelligence or other information which supports the need to locate these individuals (such as a court warrant having been issued for their arrest); *and*
  - b. a policing decision is made as to the prospects of locating them through the use of LFR.
3. the selection of images for an LFR Watchlist requires the MPS to lawfully hold them, and the MPS to have undertaken reasonable measures to ensure that the image selected is accurate such that it could be expected to assist with locating an individual of interest to the MPS;
4. the LFR system reviews images submitted for inclusion on a Watchlist and will flag issues where the image may not be suitable; *and*
5. the Threshold can be adjusted for an Alert on the LFR system to set an appropriate tolerance to avoid unduly triggering False Alerts.

### **Adjudication**

Adjudication means that the decision to Engage a member of the public is made by an officer and not the LFR system. As previously explained, officers will use their training and experience when deciding whether an Engagement is required. Officers will also assess information from the LFR system taking account of Environmental, Subject and System Factors that may affect the likelihood that an LFR Alert means that the subject is the same person held on the Watchlist. When considering generating an Alert image for officers to review, the LFR system 'by design' automatically obscures the faces of others in that image who are not the subject of an Alert. This approach limits the level of processing where an Engagement does not occur and helps ensure relevance where it does.

### **Ongoing Watchlist accuracy**

The LFR Operator has the ability to delete images from the Watchlist and will record such action in their log. This may be necessary if a person was validly placed on a Watchlist at the point the Watchlist was imported into the LFR system but was subsequently located by LFR and dealt with by the MPS before passing the same LFR Deployment later in the day. In these circumstances and to mitigate against future Alerts being generated, the image may be removed by the Operator from

the Watchlist. In any event, the Adjudication process and the role of the Engagement Officer and LFR Operator mitigates against the likelihood of Engaging once again with that person.

#### Data Retention

Controls have been implemented to minimise impact on the wider public and those on Watchlists. The controls provide that:-

1. where the LFR system does not generate an Alert, a person's biometric data is immediately automatically deleted; *and*
2. the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:-

1. personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
2. personal data is retained beyond the 31 day period in accordance with the MPS's complaints / conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
2. in accordance with the MPS's complaints / conduct investigation policies; *and/or*
3. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

Technical systems and standard operating procedures help ensure that data is properly retained or deleted. A post-Deployment review process and associated internal audit function provides assurance in this regard.

Processing mechanisms, LFR policy and systems will be reviewed at least annually in order to ensure that the personal data held is commensurate with policing purposes

## Principle 4 Accurate and up to date

The MPS is mindful of the potential damage and distress to data subjects, organisations, and to third parties if inaccurate data is processed in any way. To mitigate this, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing. There are a number of measures and controls in place to ensure the statistical accuracy and accuracy of personal data. These are set out below.

### Statistical accuracy

The ICO has provided helpful guidance on their expectations for statistical accuracy. They note that the accuracy principle “does not mean that [the LFR] system needs to be 100% statistically accurate to comply with the accuracy principle.” The ICO does however recognise the importance of considering the accuracy of the LFR system at the outset, including evaluating claims made by the vendor. In this respect the MPS has paid close regard to the NIST findings. The MPS has published a paper entitled ‘Understanding the Metropolitan Police Service LFR System’s Accuracy and Bias Position’. This explains the steps the MPS has taken to quantify the statistical accuracy and demographic performance of its LFR algorithm. In relation to NIST, this paper notes:

*“The Met’s facial recognition system uses an algorithm from a leading vendor, NEC. The NIST Test report published in 2018<sup>1</sup> evaluated over 200 algorithms for their accuracy. Its findings state that:*

*“NEC, which had produced broadly the most accurate algorithms in 2010, 2013, submitted algorithms that are substantially more accurate than their June 2018 versions and on many measures are now the most accurate”.*”

*“In March 2017, NIST also published a Face In Video Evaluation (FIVE) report.<sup>2</sup> Unlike the other NIST Tests, the FIVE test involved the use of video footage as opposed to static images. This is of particular interest to the Met because this aligns more closely to the Met’s use of facial recognition in a ‘live’ - video context. The NEC algorithm was found to be the most accurate across the different measures with a True Positive Identification rate of 82% at a corresponding False Positive Identification Rate of 0.4%.”*

The ICO has also highlighted the importance of implementing monitoring, the frequency of which should be proportional to the impact an incorrect output may have on individuals. The higher the impact the more frequently it is that monitoring and reporting is required. Cognisant of this ongoing process, the MPS LFR Documents already provide for ongoing evaluation and a post-deployment review process for LFR Deployments on a per Deployment basis. This also offers the MPS a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS’s Facial Recognition Strategic Board which reviews the performance of the LFR system at a strategic level.

---

<sup>1</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf>

<sup>2</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf>

### Currency of Watchlist

The MPS LFR Documents provide that Watchlists uploaded to the LFR system will not be more than 24 hours old. This helps to provide increased assurance that those on Watchlists remain of interest to the MPS.

Where it has been identified that it is appropriate to add an individual to a Watchlist, technical measures are in place to cross reference data with the PNC to verify that these persons are still of interest to the MPS prior to the encrypted transfer of a Watchlist to the LFR system. This protection is part of the MPS's commitment to taking all reasonable steps possible in ensuring that personal data that is inaccurate, incomplete, or no longer up-to-date, is not made available or used as part of an LFR Deployment.

### Accuracy of Watchlist

A new Watchlist is generated for every LFR Deployment. This is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching. MPS personnel are required to have taken reasonable steps to ensure that the image is of a person intended for inclusion on a given Watchlist. Images on a Watchlist will be lawfully held by the MPS. In respect of custody images, the MPS has an explicit statutory power to acquire, retain and use such imagery (see s.64A Police and Criminal Evidence Act 1984).

Where a change to data is reported by a data subject, where possible this will be used to update the LFR system and used to avoid the data subject making multiple reports.

### Quality of Watchlist Images

The MPS LFR Documents provide guidance in relation to which images are to be considered appropriate for inclusion on an LFR Watchlist. When an image is added to a Watchlist, the LFR system assesses image quality and suitability for matching, in order to allow MPS personnel to consider and manage the risk that poor quality images might generate False Alerts.

### Distinguishing Data Subjects

The LFR system produces a Template for everyone who enters the Zone of Recognition when their face is successfully detected by the system. It is not relevant or possible to distinguish between people subject of processing as a result of their being in the Zone of Recognition.

In relation to those on a Watchlist, when an Alert is generated, the system makes data available to the System Operator and Engagement Officers regarding the Watchlist subject linked to the Alert. This data includes relevant details about why the subject is on a Watchlist, e.g. wanted by the MPS for rape. This allows Engagement Officers to distinguish between those categories of person identified in s.38 (3) DPA (where applicable) and this will help inform their action.

### The Engagement Process

The Engagement process provides an opportunity for Engagement Officers to speak with members of the public and does not automatically result in the use of any policing powers.

The process provides opportunity for Engagement Officers to consider the policing data associated with a person on a Watchlist. Where lawful, the officer is able to undertake further checks to verify the information they have, helping ascertain its continued currency and accuracy.

### MPS Policy

The MPS upholds the rights of individuals under the DPA. The MPS has policies and procedures that help to ensure that inaccurate information can be updated. This includes the MPS Privacy Notice, which provides measures that allow the public to correct inaccurate information that may be held about them.

### **Principle 5: Data is kept for no longer than necessary**

The information will be retained in line with the MPS [Retention, Review and Deletion Policy](#) and the MPS LFR Documents. These are subject to at least annual review.

MPS LFR Documents detail specific controls relating to LFR data retention. The controls help ensure that the only data retained, is that which is strictly necessary to meet the purpose of the Deployment. The controls provide that:-

1. where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*
2. the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable and in any case, within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 31 days, except where:

1. personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and/or
2. personal data is retained in accordance with the MPS's complaints/conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and/or*
2. in accordance with the MPS's complaints / conduct investigation policies; *and/or*
3. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

## Principle 6: Data security

The LFR system includes a number of physical and technical security measures. These include:

1. images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine; and
2. the LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data; and
3. that the system is physically protected when in use and securely wiped following each Deployment; and
4. that role based access controls with limited user permissions are been implemented on the system; and
5. that the LFR application is connected to mobile devices using a private access point with three levels of protection; Specific IP addressing, password access to the access point, and password access to the mobile App. The mobile App has a RESTful API and will be covered by SSL; and
6. that the Dashboard and RESTful API are secured with SSL and TLS by default; and
7. that all connections are directed through HTTPS; and
8. that a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; and
9. that technical issues with the LFR system are always dealt with by LFR System Engineers working on the Deployment.

### Further Measures

As a contingency against the LFR system failing in some way that requires the LFR Operator to wipe and reset it, the encrypted USB memory stick containing the Watchlist is retained with the LFR Operator until the end of the Deployment. This means that the LFR Operator is able to reimport the Watchlist to the rebooted LFR system, enabling the Deployment to continue.

The MPS LFR Documents outlines the actions that must be taken in the event that personal data is lost. The LFR systems security measures serve to minimise the data risks and impact arising from such a loss.

The MPS undertakes vetting checks on its personnel appropriate to their role.

The MPS LFR Documents and other relevant documents such as those relating to information security are subject of regular review.

### Security Against Unlawful Processing

The MPS LFR Documents set out the structures that enable and support lawful authorisation of LFR Deployments by the MPS. No Deployment is permitted without that authorisation. During

Deployment, command teams are required to monitor and review data processing to ensure that it remains lawful. A post-Deployment debrief and review is used to identify lessons for the future and periodic audit provides assurance.

|                         |                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------|
| Protective marking:     | Official                                                                                            |
| Publication scheme Y/N: | No                                                                                                  |
| Title:                  | LIVE FACIAL RECOGNITION: LEGAL MANDATE                                                              |
| Version:                | 3.0                                                                                                 |
| Summary:                | Outlines the legal basis for the MPS's use of overt LFR technology to locate persons on a Watchlist |
| Branch/ OCU:            | MPS DLS                                                                                             |
| Review date:            | 20 <sup>th</sup> March 2024                                                                         |

**MPS LIVE FACIAL RECOGNITION: LEGAL MANDATE**

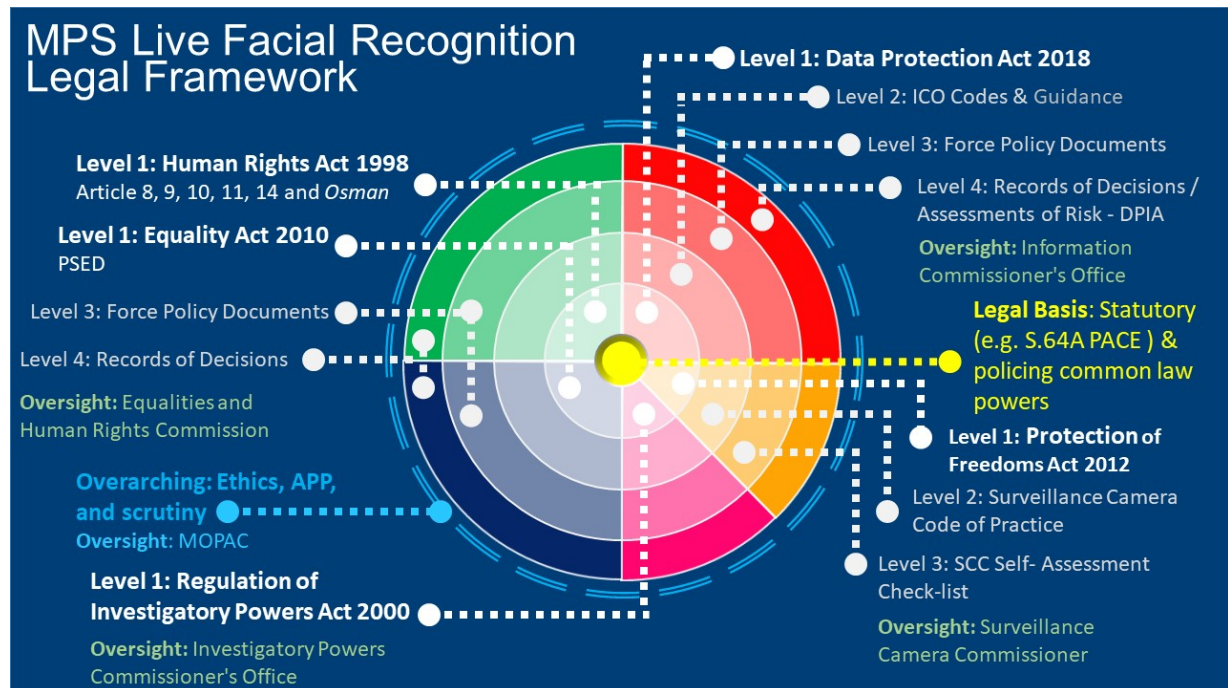
|   |                                       |    |
|---|---------------------------------------|----|
| 1 | Legal mandate .....                   | 2  |
| 2 | Legal basis overview .....            | 3  |
| 3 | Human Rights Act 1998.....            | 4  |
| 4 | Equality Act 2010 .....               | 16 |
| 5 | Data Protection Act 2018.....         | 18 |
| 6 | Protection of Freedoms Act 2012 ..... | 23 |
| 7 | Freedom of Information Act 2000 ..... | 23 |

*This legal mandate will be subject to periodic review, on at least an annual basis. It can be amended as the law and technology develops further, or as matters relating to Live Facial Recognition (LFR) evolve. It is anticipated that circumstances may arise which fall outside of the scope of this legal mandate. In such circumstances legal advice should be sought from the Directorate of Legal Services.*



## 1 Legal mandate

- 1.1 LFR for law enforcement purposes is not subject to dedicated legislation. Instead, in line with the way the Metropolitan Police Service (MPS) exercises its well-established common law and statutory powers, LFR is regulated by a number of sources of law, more particularly identified below in the schematic. These sources of law combine to provide a multi-layered legal structure to use, regulate and oversee the use of LFR by law enforcement bodies (the LFR Legal Framework).



- 1.2 The legal framework schematic is best read from the inside of the diagram out in the following way:

| Legal Framework Schematic Key: |                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Yellow centre</b>           | This is the legal basis for the action – i.e. the legal power(s) that supports the compilation of the Watchlist and the use of LFR.                                                                                                         |
| <b>Red segment</b>             | This area reflects that biometric and other personal data is processed by the LFR system. It reflects the application of the Data Protection Act 2018 and underlying documents that govern and reflect this.                                |
| <b>Green segment</b>           | This area reflects the relevance of human rights to the use of LFR. Some, like the right to privacy, will be engaged by those on the LFR Watchlist and/or passing the LFR system. The engagement of other rights will be context dependant. |
| <b>Blue Segment</b>            | This area reflects the relevance of equality considerations and the application of the Public Sector Equality Duty. It shows the underlying documents which also govern and show compliance with this duty.                                 |
| <b>Pink Segment</b>            | This area reflects the potential application of the Regulation of Investigatory Powers Act 2000 (RIPA). For an overt capability, it is important to have regard to RIPA to ensure the use of LFR does not become directed surveillance.     |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Orange Segment</b> | This area reflects that LFR uses CCTV cameras to film those passing through the Zone of Recognition as part of the wider LFR system. It recognises the relevance of the Protection of Freedoms Act 2012 to CCTV in public spaces by policing in England and Wales.                                                                                                                                                                                                                                                                                                                                       |
| <b>Level 1</b>        | <b>Primary legislation:</b> This level of the legal framework reflects a statutory legislation enacted by Parliament that combines in its application to provide a framework for the regulation of LFR.                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Level 2</b>        | <b>Secondary legislative instruments:</b> This level of the legal framework reflects statutory codes and non-statutory guidance typically issued at a national level which Chief Officers should have regard to when seeking to apply the Level 1 legal framework.<br><br>Authorised Professional Practice (APP) issued by the College of Policing also sits at this level within the legal framework. However, given some APP is not specific to a particular area of primary legislation, it is reflected as an overarching consideration in the legal schematic to reflect its pervasive application. |
| <b>Level 3</b>        | <b>Force policy:</b> This reflects policy documents issues at a force level. They provide for the operational implementation of the legal framework in a way that helps the use of LFR to be both accessible and foreseeable to the public.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Level 4</b>        | This level of documentation reflects the use of the legal framework in practice – ensuring relevant decisions, including the rationale, necessity and proportionality for use is recorded. It is also the place where decisions of relevance to the Public Sector Equality Duty should be recorded.                                                                                                                                                                                                                                                                                                      |
| <b>Overarching:</b>   | The all-encompassing <a href="#">blue dashed line</a> shows that there are a number of aspects to the lawful and ethical use of LFR systems which are pervasive and do not just relate to one area of law.                                                                                                                                                                                                                                                                                                                                                                                               |

## 2 Legal basis overview

- 2.1 Common law: As a police service, the MPS has a number of long established policing responsibilities and powers derived from the common law which have been consistently recognised by the courts. The MPS is obliged to comply with the common law and statutory safeguards in delivering its policing operational duties and relies on the common law to discharge a number of its duties.
- 2.2 Key common law powers the MPS may rely on when utilising LFR technology include the policing common law powers to:
- (a) protect life and property;
  - (b) preserve order and prevent threats to public security;
  - (c) prevent and detect crime;
  - (d) bring offenders to justice; *and*
  - (e) uphold national security.

**Example:** The MPS has identified uses for LFR as a tool for locating those who have outstanding warrants for their arrest for knife and gun crimes. In this context, the use of LFR technology to facilitate officers to promptly locate those evading arrest would enable the MPS to discharge its responsibilities to protect life and property. It would also be compatible with the MPS's duty to bring offenders to justice by facilitating a prompt and effective investigation.

- 2.3 The use of the police's common law powers as a legal basis to support the deployment of LFR are considered further in relation to human rights below. The common law powers have also been considered and recognised in the 'Bridges' case:
- (a) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) (the "High Court Bridges" decision); and then on Appeal in,
  - (b) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision).
- 2.4 Watchlists: The Court of Appeal further summarised the legal basis in relation to compilation of Watchlists as being "both authorised under the Police and Criminal Evidence Act 1984 and within the powers of police at common law." The reference to the 1984 Act is a reference to imagery obtained pursuant to Section 64A (*Photographing of suspects etc.*) and particularly section 64A (4) (a). This allows a photograph taken under the section to be "used ... for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence". The Court of Appeal notes that "this was not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy [LFR]."

**Key point for Authorising Officers:** When considering the use of LFR technology, MPS Authorising Officers should be clear as to the legal basis the MPS relies on for lawful authority to deploy LFR and record this as part of the decision making process.

### 3 Human Rights Act 1998

- 3.1 The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Rights (ECHR) into domestic British law.
- 3.2 All MPS use of LFR will comply with the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

*"There 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 well-being 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."*

- 3.3 As a qualified right, any interference with an individual's Article 8 rights is only permissible if:
- (a) there is a legal basis for the interference with the qualified right that the public can understand;
  - (b) the use of LFR seeks to achieve a legitimate aim;
  - (c) it is necessary for the purposes of that aim in a democratic society; *and*
  - (d) the use of LFR is proportionate to the legitimate aim being sought.
- 3.4 It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom*<sup>1</sup> confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that LFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".<sup>2</sup>
- 3.5 The High Court and Court of Appeal Bridges cases further considered Article 8, specifically in the context of facial recognition and has confirmed that Article 8 is engaged in so far as someone passes an LFR system and in so far as someone is placed on a LFR Watchlist for a Deployment. Depending on the nature of the Deployment, the then Surveillance Camera Commissioner has identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. The Directorate of Legal Services has further advice available for Authorising Officers should they consider a proposed Deployment may have wider human rights points to consider.
- 3.6 There is a legal basis for the interference with the qualified right that the public can understand.

LFR will be used to allow the MPS to discharge its well-established operational duties pursuant to common law. The courts have recognised that "the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them".<sup>3</sup>

In the case of *R (Catt) v Chief Police Officers [2015] A.C. 1065*, Lord Sumption recognised that applicants could have their personal information noted down and retained by the police as they occupied publically accessible space. The court recognised the police's common law powers to collect and store information are subject to an "intensive regime of statutory and administrative regulation" under the Data Protection Act and various guidance documents on the management of police information.

The courts have further recognised the right of the police to make use of a photograph of an individual. The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect's accomplice or of anyone else. The court confirmed the "key is that they must have these and only

---

<sup>1</sup> (2009) 48 EHRR 50, at [66 and 67]

<sup>2</sup> At [104]

<sup>3</sup> *R (Catt) v Association of Chief Police Officers [2015] A.C. 1065* at [11].

these purposes in mind and must ... make no more than reasonable use of the picture in seeking to accomplish them”.<sup>4</sup>

- 3.7 In the case of the MPS’s use of LFR, the LFR Legal Framework provides the legal basis for any interference with an individual’s Article 8 rights. The High Court Bridges case confirmed the police’s common law policing powers to be “amply sufficient” in relation to this type of use of LFR and confirmed that “the police do not need new express statutory powers for this purpose”. This was further considered in the Court of Appeal Bridges case which also recognised the sufficiency of the legal framework, noting<sup>5</sup>:

*“the legal framework which regulates the deployment of [SWP’s use of LFR] does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined.”*

- 3.8 The Court of Appeal Bridges decision further noted that, to be ‘in accordance with the law’ the legal basis must:

*“be ‘accessible’ to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be ‘foreseeable’ meaning that it must be possible for a person to foresee its consequences for them and it should not ‘confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself’.”*

- 3.9 In considering accessibility and foreseeability, the Court of Appeal examined the level of discretion that South Wales Police officers held to determine *where* they deployed facial recognition technology and *who* they deployed it to locate. The court refers to this as the “Who Question” and the “Where Question”.

- (a) The ‘Who’ Question: When considering how the ‘Who Question’ should be answered, the Court of Appeal made it clear that, the law does not seek specific confirmation as to who is on a Watchlist (they recognise the NCND principle<sup>6</sup>). The Court of Appeal recognised that individuals could be added to a Watchlist on the basis that they are wanted on suspicion of an offence, wanted on warrant and vulnerable persons”.
- (b) The Court of Appeal also explains why a category of those “other persons where intelligence is required” was not accessible and foreseeable to meet the ‘in accordance with the law’ test. They noted that the category was not readily understood, nor was it objective – it left “too broad a discretion vested in the individual police officer to decide who should go onto the watchlist” – essentially it allowed police officers to decide what ‘other persons where intelligence is required’ meant on a case-by-case basis rather than deciding if a subject met the criteria set out in the force policy.
- (c) Following an approach recognised by the Court of Appeal<sup>7</sup>, the MPS addresses the ‘Who Question’ in its published MPS LFR Documents, particularly at Section 6 of the MPS LFR SOP. The MPS sets the criteria that applies to govern the images that may be included on a

---

<sup>4</sup> Per Laws J in *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 at 810F

<sup>5</sup> At [69].

<sup>6</sup> At [95].

<sup>7</sup> At [118].

Watchlist and in what circumstances. To ensure the Watchlisting criteria is accessible and foreseeable, the MPS explains terminology such as ‘presenting a risk of harm’ and ‘otherwise of interest to the police’ such that they can be readily understood and objective to both officers and the public. It sets out the standard required for inclusion on a Watchlist, linking the necessity and criteria for the inclusion on a Watchlist with the policing need and the proportionality of taking any action.

- (d) The ‘Where Question: The Court of Appeal noted that the South Wales Police team “was not able to draw to our attention anything which specifies where AFR Locate may be deployed”. The MPS LFR Documents answers this question, particularly the MPS LFR SOP at Section 5. In answering this question, in many instances, the need to locate a person will determine where it is best to site LFR to facilitate making a successful location. However, other factors will also be relevant and these include the nature of the site itself from a privacy perspective, those passing the site, and the policing need to be at the site (including for the public’s protection, suppressing crime hotspots, and getting ahead of crime trends).

With the benefit of the *Bridges* decisions, the law has now been applied to the live use of facial recognition technology. These judicial decisions, taken together with the MPS’s published documentation to support the use of LFR allows the LFR Legal Framework principles to be predictably applied to the use of LFR in an accessible and understandable way. It allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the MPS operates to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

### 3.10 The use of LFR seeks to achieve a legitimate aim.

Article 8, recognises action in the interests of national security, public safety and the prevention of disorder or crime as legitimate aims. The use of LFR in the context of fighting crime including knife and gun crime, child sexual abuse and exploitation (including online) and terrorism offences will help the MPS to achieve its law enforcement purposes.

The means by which the MPS may use LFR will be an operational decision within the parameters of the law and the MPS LFR Documents. It will need to be driven by the policing issue at hand. This may vary from the need to locate those wanted in connection with criminality or otherwise pose a risk of harm, to more preventative tactics designed to bring reassurance to communities and enable the use of precision technology to more proactively focus policing resources.

**Key point for Authorising Officers:** At the point that it is decided to deploy LFR, the decision maker should be clear as to its purpose and how using LFR will help the MPS realise a legitimate aim. In deciding if the use of LFR is a suitable way to achieve a legitimate aim, the decision maker should consider if benefits of using LFR justify its use for that legitimate aim when compared to any impact on an individual’s Article 8 Rights.

### 3.11 The use of LFR is *necessary* for the purposes of that legitimate aim in a democratic society

Necessity is a demanding requirement to justify any interference with Article 8. It requires the action to lie somewhere between “indispensable” and more than something that is merely “desirable”. In this respect, LFR will be used in response to a pressing social need by helping the MPS to fight crime in areas where LFR has the greatest potential to assist. It is a tool that helps the MPS to discharge its operational responsibilities, primarily to help it prevent and detect crime.

**Key point for Authorising Officers:** When considering the Deployment of LFR, its use is to be underpinned by an intelligence case to highlight the need to combat the relevant crime issue or policing need to deploy. Having identified a need, this will then allow Authorising Officers to consider the use of LFR. Authorising Officers need to decide the use of LFR is *necessary* and not just desirable to enable the MPS achieve its legitimate aim. In deciding if the use of LFR is necessary, consideration should be given to the intelligence case as this will be important in outlining the need to deploy to a particular location and the composition of the Watchlist. Consideration should also be given to whether there is an alternative, including the viability and intrusiveness of any alternative.

Authorising Officers need to keep a record why they considered the use of LFR to be necessary, the issue which LFR was intended to address and how LFR would be deployed to address that problem. This rationale should also explain how the intelligence case justified the Deployment location and Watchlist composition as being necessary in order to enable the MPS to pursue its legitimate aim.

The following are examples of why LFR may be used as a necessary tool to assist the MPS in preventing crime and disorder. The examples are illustrative only and there will be other scenarios where the use of LFR is justified.

**Terrorism example:** The use of LFR will assist the MPS in fighting terrorism. By way of example, LFR could be deployed at international borders. This can be part of tailored security measures to keep people safe as LFR can act as a valuable tool to assist police officers to identify those of interest to the police for terrorism reasons including those who may be travelling on false documentation. LFR therefore supports officers who have the challenge of being familiar with a potentially significant and rapidly changing number of persons who are often motivated not to be identified and where the consequences of a missed identification opportunity can be catastrophic. Using LFR in this way would help the MPS achieve its aim of preventing crime and disorder and protecting the public through the disruption of those seeking to commit terrorist offences by making it harder to travel undetected across borders.

**Child sexual abuse and exploitation example:** The use of LFR will assist the MPS in fighting child sexual abuse and exploitation. LFR could be deployed based on intelligence to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse and exploitation. Missing person investigations use significant police resources where the need to locate and make an identification is often time critical. In such circumstances, it is of great importance to use all reasonable measures, to have the best chance of making a successful identification when the often scarce identification opportunities arise. At times, the police may also enlist the public to help with locating missing people through the use of public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use LFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers the MPS a route to discharge its common law responsibilities to protect life.

Additionally, in a climate where police forces need to operate efficiently, the MPS has also identified that technology such as LFR can assist with the challenges of quickly and cost efficiently locating those with outstanding warrants or who have otherwise breached their bail conditions. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances. The High Court Bridges case supports that there is a "considerable additional benefit to the public interest to including those wanted on a warrant" for a Deployment of LFR, even when there is no specific intelligence to place them in the area of the Deployment. The intrusion to those passing the system is no greater, but (i) the potential to protect the public from those wanted by the courts, (ii) the results from Deployments where those with outstanding warrants were included and (iii) the resultant arrests justified the inclusion of those with outstanding warrants from the courts as a *necessary* action to bring offenders to justice.

### 3.12 The use of LFR is *proportionate* to legitimate aim being sought

When considering the Deployment of LFR, the benefits of using LFR for an investigation or operation should not be disproportionate or arbitrary. In this respect, the Surveillance Camera Commissioner recognises that:

*"used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".*

In this respect, the following factors (amongst others, depending on the nature of the Deployment) will guide Authorising Officers:

- (a) *The use of LFR should be a reasonable use of MPS powers - it will not be proportionate if the proposed use of LFR is excessive in the overall circumstances of the investigation, operation or wider operational strategy to tackle a policing issue.*

Authorising Officers will need to consider the seriousness of the policing issues at hand and the potential benefits of using LFR and balance this with any wider impact its Deployment may have to those on a Watchlist and the public at large. This will allow a decision to be made as to whether LFR is appropriate for use. Authorising Officers must consider the composition of the Watchlist compiled for the LFR system to match against, to ensure that it is not



compiled in an excessive manner. The Watchlist needs to satisfy the necessity and proportionality test and will therefore be driven by the intelligence case and bespoke for the Deployment of LFR to ensure it meets the aims of each Deployment. With this in mind, the Watchlist compiled for each Deployment of LFR should be current; based on those currently of interest to the MPS and/or wider UK law enforcement to mitigate the risk of the LFR system matching with those no longer of interest to the MPS and/or wider UK law enforcement.

- (b) *Consideration should be given as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference.*

The use of LFR should be considered against other methods of locating persons of interest to the MPS and/or UK Law Enforcement and other policing tactics which may help tackle the policing issue at hand. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation or Deployment.

**Example:** Circulating a wanted image on social media may be considered as an alternative to the use of LFR.

The use of LFR can be targeted to a specific area and does not result in the public being made aware of the identity of a person being sought by the MPS. It can also be used for a limited period, targeted, based on wider intelligence, to times and places when it might be most expected to locate an individual.

By comparison, social media results in a person's image being put into the public domain in a less targeted way. Once online, the image is public and the MPS no longer has control of that image. It therefore has potential to remain online even when the person has been traced and thus is a greater intrusion into the privacy of the individual being sought.

The Authorising Officer considering the use of LFR should balance any intrusion into privacy against the need for the investigative activity. If the Authorising Officer uses LFR in a way that minimises any impact it may have on a person's privacy as far as possible, it may offer a more appropriate, less intrusive alternative to a social media campaign.

**Key point for Authorising Officers:** When taking a decision to deploy LFR, Authorising Officers should record what other methods, as appropriate, were either not implemented or have been employed but which were assessed to be insufficient or inappropriate to fulfil the MPS's aim.

- (c) *How and why the methods adopted will cause the least possible inference to the person(s) sought and others must be addressed.*

All uses of LFR under this Legal Mandate will be overt. LFR will be used for a limited time – with a limited footprint, with a defined purpose (controlled by way of the MPS LFR 1 Form and the MPS LFR Documents). The LFR system will be visibly deployed in an open and transparent way. Consistent with the principle of engaging with the public, the MPS LFR

Documents also provides a structure for awareness measures which respond to the nature and objectives of the use of LFR.

**Key point for Authorising Officers:** When considering the use of LFR, Authorising Officers will need to assess and minimise any impact on those who pass the LFR system to manage and mitigate any collateral intrusion.

**Proportionality controls.** Controls are also designed in to the LFR system and its operation to help minimise any impact on the public and those places on a Watchlist as follows:

1. LFR cannot be used to locate persons unless they have been included on a Watchlist.
2. The creation of any Watchlist is specific to the Deployment of LFR and informed by the intelligence case for the Deployment; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching.
3. Images on a Watchlist will be lawfully held by the MPS with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Watchlist.
4. Authorising Officers need to expressly consider and approve the use of non-police originated images on any Watchlist. This is because particular privacy considerations may attach to an image where it originates from outside of a policing context. For example, it may be that the image was not placed in the public domain, was taken in a place that attracts a higher expectation of privacy or is an image that was supplied to, or taken by a third party for a specific purpose that does not usually see routine data sharing with the police. Even when the MPS can lawfully hold the images, the need for the Watchlist to be a proportionate policing response requires the Authorising Officer to undertake a careful assessment of an individual's privacy expectations against the policing need to locate them using LFR. The MPS LFR SOP outlines considerations for Authorising Officers at Section 6.
5. On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate LFR Alerts.
6. All Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.
7. The cameras used in the LFR system are of sufficient quality for the LFR system's needs.
8. The LFR system is 'closed' and not connected to other MPS systems or the internet.
9. The LFR system is designed to assist MPS personnel locate people. The LFR system will always flag potential matches to at least one officer for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.
10. When the LFR system flags a match to MPS personnel, the context picture obscures the faces of all those passing the LFR system other than the person who generated the Alert.
11. LFR Deployments and the materials that support LFR Deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

Controls have also been implemented with regards to personal data retention to minimise the impact on the wider public and those on the Watchlist. The controls provide that:

1. where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; and
2. the data held on the encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.

Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:

1. personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and/or
2. personal data is retained in accordance with the MPS's complaints / conduct investigation policies.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
2. in accordance with the MPS's complaints / conduct investigation policies; and/or
3. in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

**Deployment location privacy considerations.** Many Deployment locations will be identified as being necessary by the intelligence case supporting the prospects of locating persons at the site and/or how LFR plays a role within wider policing tactics. However, Authorising Officers must also consider the reasonable expectations of privacy the general public may have as a whole when traversing a public place where LFR is being considered for Deployment. Some places, and the people expected to be at some places by their nature attract greater privacy expectations than others. Authorising Officers also need to consider what measures are appropriate to identify the use of LFR when it is deployed, particularly where expectations of privacy may be greater. This is important to establishing if the proposed use for LFR, and the Deployment location itself is proportionate.

**Example:** The public's expectations of privacy will be different in different public spaces. In Central London, the public has historically been protected by initiatives such as the 'ring of steel'. The public is also accustomed to an extensive use of similar systems such as CCTV, police patrols and other crime fighting/public safety systems deployed in order to ensure public safety. By comparison, there could be a higher expectation of privacy in a quiet outer London suburban street, albeit the public would still expect the police to conduct investigations to prevent and detect crime. The use of LFR may also be more expected in areas that have high rates of crime where police action would be more expected.

Authorising Officers should also consider if a proposed Deployment location attracts particular privacy concerns by reference to those expected to be at a particular location.

**Example:** Areas particularly focused on providing facilities or attractions aimed at children would typically attract greater privacy expectations over an area that typically sees attendance from the public more broadly. The public would not typically expect LFR to be sited outside a toyshop or school that may disproportionately see children passing the LFR system if the LFR system could be sited elsewhere. There may nevertheless be instances where the intelligence case, and the need to protect children makes it necessary and proportionate to deploy LFR to these areas. For example if it is known that wanted sex offenders are targeting those that visit the location and it not possible to locate them by siting LFR elsewhere or using other less intrusive policing tactics. If it is necessary to use LFR at the location, mitigations to reduce the privacy impact should be used wherever possible. This could include extra measures to ensure that the signage and information about the LFR Deployment is accessible to children who pass through the Zone of Recognition. Where it is possible to so, and does not increase the risk to children, the time of a Deployment and configuration of a Zone of Recognition should also seek to minimise the numbers of children assessed by the LFR system.

Areas assessed as having high expectations of privacy which give the public little option to avoid the LFR area without substantial inconvenience should generally be avoided unless the following mean that the Authorising Officer is satisfied the use of LFR in the circumstances remains necessary and proportionate:

1. the importance of using LFR in that location to realise a legitimate aim supports LFR's use;
2. the lack of a viable, less intrusive alternative available for use in the circumstances;  
*and*
3. any further mitigations to reduce any impact to the wider public in so far as it is possible to do so.

**Example:** If there was a necessity and proportionality case, based on intelligence, to deploy LFR in a residential area to locate a group of violent robbery offenders, then we understand there may be a greater expectation of privacy in this area. To mitigate this, depending on the circumstances we may provide additional communication about the use of LFR, for example by posting on local neighbourhood social media groups.

**Key point for Authorising Officers:** When taking a decision to deploy LFR, Authorising Officers should record the measures taken to ensure the use of LFR causes the least possible interference to the person(s) sought and others. This should include explicit reference to any particular privacy considerations that may be relevant to a Deployment location and any mitigations in place to reduce the impact of the LFR Deployment on the wider public. Authorising Officers should then continue to review Deployments of LFR to ensure the use case remains appropriate.

### 3.13 Wider Human Rights Act considerations

The right to privacy is a value which protects the autonomy and human dignity of individuals by enabling them to conduct their lives in a way of their choosing. There are therefore circumstances when freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and of association (Article 11) may be particularly relevant.

- (a) *Article 9.* The clothing people wear can be an act of thought, conscience and religion and in normal circumstances, the police do not have the legal power to require a person to remove clothing (including any headwear) simply because they are passing the LFR system. Additionally, the location where people may pass the LFR system may also engage Article 9.

**Example:** The use of LFR can assist the MPS to ensure public safety, including at a place of worship where the intelligence case has identified a threat to the public. A decision to place a LFR Deployment outside a place of worship or in a way that substantially impedes access to a place of worship can engage Article 9. In this context, the public safety considerations need to be balanced against the need to use LFR at that location. If the public safety policing objectives could be achieved by deploying the LFR system elsewhere, it would not be necessary to deploy LFR at the proposed location. If the threat that makes it necessary to site LFR near to a place of worship, Authorising Officers also need to determine if the infringement on Article 9 rights is disproportionate to the likely benefits of using LFR. Considerations would typically include the impact on those seeking to access a place of worship, the likely impact on the same people without LFR (being potentially impacted by other policing measures or site closures) and the benefits to safety LFR brings the public.

- (b) *Article 10 and 11* have particular relevance when considering both the policing of assemblies and demonstrations and any use of LFR which may impact on an assembly or demonstration. Article 10 is especially pertinent should people have reservations about expressing themselves as a result of an LFR Deployment. Article 11 is also relevant should the use of LFR deter people from attending an assembly or demonstration at all or otherwise cause people to minimise their involvement.

**Example:** The use of LFR can assist the MPS in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. In deciding the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights and the risks of having a 'chilling effect' on the exercise of such rights. There may be expectations of anonymity in a crowd and individuals may choose to alter their means of demonstration because of the LFR Deployment. Article 10 and 11 rights must be weighed against the need to use LFR to enable an assembly that might otherwise be disrupted by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of LFR. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety. They could also include there being focus placed on ensuring the public understand the use of LFR is to help them safely undertake their assembly.

- (c) *Operational Duties.* The 'operational duty' was first outlined in the case of *Osman v United Kingdom*<sup>8</sup> and concerned an alleged failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights in *Osman* found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Case law also supports that the police are under an *Osman* style duty to investigate serious allegations in a timely and efficient manner in order to uphold an individual's Article 3 rights.<sup>9</sup>

The *Osman* operational duty has particular relevance to LFR in two contexts (i) being used to locate those posing a threat to the public or themselves where a real and immediate risk to life is identified and LFR is thought to provide an appropriate response to such risk and (ii) on an Alert being generated where the need to locate that person may engage the *Osman* operational duty with measures being put in place should a person generating an Alert seek to evade officers.

- (d) *Article 14.* This right requires that all of the rights and freedoms set out in the Human Rights Act 1998 must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and have equal access to them. Article 14 is not a stand-alone right – there is a need to show that discrimination has affected the enjoyment of one or more of the other human rights, not that the other rights have actually been breached. The use of LFR will be relevant in circumstances where demographic performance of the LFR algorithm varied to such an extent that people of a particular demographic were more or less likely to see a False Alert generated against them. As a result there are two points to consider in relation to the MPS LFR system (i) does the LFR system's demographic differential performance vary by a particular demographic such as it results in a person suffering a discriminatory effect and (ii) if there is a difference in treatment, is this capable of an objective and reasonable justification<sup>10</sup>. In relation to an objective justification, the questions to ask are (i) does LFR

---

<sup>8</sup> [1999] 1 F.L.R. 193 (ECtHR)

<sup>9</sup> *Commissioner of Police of the Metropolis v DSD and another* [2018] UKSC 11

<sup>10</sup> *Molla Sali v. Greece* [GC], 2018, § 135; *Fabris v. France* [GC], 2013, § 56; *D.H. and Others v. the Czech Republic* [GC], 2007, § 175; *Hoogendijk v. the Netherlands* (dec.), 2005.

pursue a legitimate aim and (ii) are the means employed reasonably proportionate to the aim pursued?

1. **LFR system performance:** In relation to the performance of the MPS LFR system, the MPS has published a paper titled 'The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences'. This provides assurance regarding demographic performance and explains the steps the MPS has taken to understand the statistical accuracy and demographic performance of its LFR algorithm. Further details are also outlined in relation to the Equality Act 2010, below.
2. **Legitimate aim:** Article 14 does not prohibit differences in treatment that are based on a public interest. What constitutes a legitimate aim is an area where case law continues to develop with the courts having recognised a wide range of purposes including a number of actions within the ambit of criminal justice.<sup>11</sup>
3. **Proportionality:** After establishing a legitimate aim, the Court requires that the difference in treatment should strike a fair balance between the protection of the interests of the public and respect for the rights and freedoms of the individual. Assessing the balance struck, the court will afford a margin of appreciation to reflect the expertise of the public body. Paragraph 3.12 of this Legal Mandate outlines further considerations in relation to proportionality and in particular reflects (i) the selection of a high performing algorithm, (ii) the importance of the policing purpose, (iii) the safeguards and controls implemented to ensure the use of LFR causes the lowest possible intrusion whilst still achieving the legitimate aim.

#### 4 Equality Act 2010

- 4.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination based on different treatment on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, the MPS must comply with section 149 of the Equality Act 2010 that is most commonly known as the Public Sector Equality Duty ("PSED").
- 4.2 The MPS is required to take measures to ensure that the use of LFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of the LFR system (and then, if performance varies by any particular demographic), and (b) the operational Deployment of the LFR system:

(a) *The technical performance of the LFR system.*

The Court of Appeal Bridges decision makes it clear that the PSED requires the MPS to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias on grounds of race or sex. To assist the public with understanding how the MPS meets its PSED duties, the MPS has

---

<sup>11</sup> Restoration of peace - *Sejdić and Finci v. Bosnia and Herzegovina* [GC], 2009, § 45 and protection of national security - *Konstantin Markin v. Russia* [GC], 2012, § 137)

published the MPS LFR Equality Impact Assessment. Additionally, the MPS has published a paper titled 'The Metropolitan Police Service Facial Recognition Technology: Understanding accuracy and demographic differences' 'This explains the steps the MPS has taken to understand the statistical accuracy and demographic performance of its LFR algorithm. This includes:

1. **Independent evaluation:** A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result, the MPS has paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by the MPS. The MPS has then taken this further with the National Physical Laboratory (NPL) who have undertaken a scientifically underpinned evaluation of the MPS's LFR algorithm in the operational environment and published their conclusions as regards the MPS LFR algorithm's performance. The MPS has then reflected the findings in the MPS LFR Documents to inform its operational practice.
2. **Peer review:** The MPS's position paper has been reviewed by other experts in the field including the Defence Science and Technology Laboratory and the National Physical Laboratory.
3. **Ongoing assurance:** The MPS LFR Documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and also offers the MPS a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS Facial Recognition Strategic Board.

*(b) The operational Deployment of the LFR system.*

The MPS LFR Documents are also responsive to the Subject, System and Environmental Factors to ensure the LFR system is suitable for its intended use and operating correctly. Subject, System and Environmental Factors including aspects such as camera configuration, camera location, lighting conditions, the distance at which people will pass the LFR system, crowd flow levels in so far as this may result in occlusion (including by reference to the height of the subjects being sought) and points relating to an individual's age and appearance have been considered carefully in the MPS LFR Documents to ensure the efficacy of the LFR system and the MPS's compliance with its Equality Act 2010 duties.

By way of example, the MPS LFR Documents provide that LFR Operators are trained to identify Watchlist issues with proposed images which may impact on system performance. Where the need to use an image is deemed to be necessary and proportionate, those using the LFR system have received training to maximise the LFR system's performance and to effectively consider any issues arising from the use of such images as part of the identification process.



As a result of having taken reasonable steps to understand the statistical accuracy and demographic performance of the MPS LFR system and then in light of points relating to Subject, System and Environmental Factors and the framework of safeguards implemented as a result, the MPS has adopted a 'fail-safe' position to ensure that absent there being other lawful grounds to take policing action:

**No Engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own opinion that there is a probable match between the member of the public and the Watchlist image.**

This means the LFR system is not making any decision to Engage with the public, the officer is making this decision - just as officers make similar decisions to Engage with members of the public every day (without the support of LFR). The officer is best placed to make this decision, drawing on their training and policing experience.

Similarly, the officer is best placed to consider the impact of any Subject, System and Environmental Factors that may have influenced the LFR system when it generated an Alert and if such factors combine to mean an Engagement with a member of the public is not appropriate in the circumstances.

**Key point for Authorising Officers:** In order to ensure that the officer is best able to make an informed decision on any Engagement, all officers who are part of an LFR Deployment are to have been briefed on the operation of the LFR system. This includes Subject, System and Environmental Factors that can impact performance. LFR Engagement Officers should also have been given training relating to unconscious bias given their key role in the Engagement decision-making process.

Beyond Subject, System and Environmental factors, MPS personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of other crime fighting techniques, for example, 'stop and search'. In this respect, it is important that the use of LFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment and, where relevant, the Community Impact Assessment informs the policing plan to support the Deployment of LFR to mean the MPS upholds the Public Sector Equality Duty. Compliance with the Equality Impact Assessment should then be monitored and reviewed for the duration of that Deployment.

## **5 Data Protection Act 2018**

- 5.1 The MPS processes personal data for LFR 'based on law'; specifically its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate, and the policies put in place by the MPS LFR Documents. The Appropriate Policy Document and other MPS LFR Documents published by the MPS as a public body allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the MPS operates to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

- 5.2 For the purposes of preventing crime and disorder, Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including sensitive processing, whether processed on a computer, CCTV, still images or other media. Any recorded image from a device that can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR both in terms of locating those on a Watchlist but also in terms of processing biometric information of members of the public to confirm they are not on a Watchlist. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

*"For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."*

**Key point for Authorising Officers:** Authorising Officers already need be satisfied of the necessity to use LFR to prevent crime and disorder and ensure public safety in the context of the Human Rights Act 1998. Similarly, to satisfy Section 35(5) DPA, they need to be content that the LFR system's processing of biometric data is strictly necessary for the law enforcement purpose. The law enforcement purpose should be clearly identified and the way in which the strictly necessary standard has been met explained.

- (a) Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via LFR is not used in a manner that is contrary to the identified law enforcement purpose.

**Example: alternative policing methods to prevent threats to public security:** LFR may be deployed to police a high profile well-attended public event. When considering alternatives, in this example, other measures such as extra CCTV may be considered. However, they will not always be a viable less intrusive alternative in the circumstances. For example:

1. Whilst CCTV can help ensure event safety, it lacks the ability to actively Alert officers to the potential presence of individuals of interest to them.
2. It may not be practical to expect officers to recognise larger numbers of people of interest to the Police given the nature and scale of the event, the numbers of officers available to police the event and the flow rate and number of people passing the CCTV system. This is especially relevant where the importance of making such identifications supports the use of a more suitable alternative such as LFR.
3. Where LFR is thought to offer further important protection to the public as opposed to other policing methods. For example, this may apply where the law enforcement purposes for a Deployment include wider public safety considerations. These may include the need to locate those wanted by the courts. Such persons may attend such a high profile event and, in line with the decision of the courts to require their arrest, pose a risk to the public generally.

- (b) The 'strictly necessary' standard may be informed by the Authorising Officer considering factors including:
- (i) what other policing methods (including those that do not require sensitive processing to be undertaken) have been used / discounted when seeking to

- locate an individual(s) on the Watchlist or to provide a series of tailored security measures;
- (ii) the importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose through the Deployment of LFR at the proposed location with the proposed Watchlist (for example, is the Deployment intelligence-led or otherwise supported by information which confirms that LFR can be expected to get results in the circumstances being contemplated);
  - (iii) the size and scale of the planned LFR Deployment and associated Watchlist and the level of sensitive processing anticipated as a result of the LFR Deployment; and
  - (iv) if the law enforcement purpose which underpins the use of LFR is strictly necessary and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

**Key point for Authorising Officers:** Authorising Officers need to be satisfied that the processing satisfies one of the Schedule 8 conditions set out below and complies with the six data protection principles.

### 5.3 Schedule 8 conditions of the DPA are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; *and*
- necessary for archiving, research or statistical purposes.

**Example:** The use of LFR will assist the MPS in fighting knife and gun crime in support of its common law policing powers. LFR could be deployed to identify wanted offenders who have failed to comply with court bail relating to such offences. Used in this way, LFR would assist in the prevention, investigation, detection or prosecution of criminal offences.

LFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description to scan a crowd and try to spot an offender where positive results would otherwise be less likely and the risk of people being missed, higher. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context, to enable the MPS to effectively respond to a pressing social need, LFR's use may be seen as strictly necessary to support the investigation of knife and gun crime.

Similarly, the Schedule 8 condition of being necessary for judicial and statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe. For similar reasons, the court in the Bridges cases accepted the substantial public interest in the police using LFR to discharge their common law policing duties.

5.4 The MPS has also undertaken a number of steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the LFR system. Particular actions are set out in the remainder of this section.

5.5 Data Protection Impact Assessment:

A DPIA has been conducted to support the use of LFR in order to identify and minimise the data protection risks. Whilst the overall DPIA will be reviewed annually, Authorising Officers authorising the use of LFR should ensure there is a DPIA in place that is sufficient for each Deployment. Specifically, consideration should be given to:

- (a) if the risks and controls remain current and sufficient for the planned use of LFR; and
- (b) if the planned use for LFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.

5.6 Data Protection by Design:

A number of data protection controls have been designed into the LFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into LFR processing activities. The designed-in measures identified at paragraph 3.12(c) of this document, include measures to:

- (a) limit the amount of personal data collected;
- (b) limit the extent of personal data processing;
- (c) limit the period of personal data storage.

Additionally, the MPS has acted to ensure that the LFR system performs to a level where the statistical accuracy of the data being processed and fairness 'by design' is ingrained into the MPS's LFR system. The MPS LFR Documents and other published supporting information explain how the MPS is assured that its LFR system operates with a sufficiently high degree of statistical accuracy – such that it can achieve the legitimate aim in a way that does not lead to unjust results between demographics.

Further consideration has been given to limiting access to any personal data retained for the 31 day period. The LFR system also includes a number of physical and technical security measures including:

- (a) Images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine;
- (b) The LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data;
- (c) The LFR system is physically protected when in use and securely wiped following each Deployment;
- (d) Role based access controls with limited user permissions are implemented on the LFR system;
- (e) The LFR application is connected to mobile devices using a private access point with three levels of protection (i) specific IP addressing, (ii) password access to the access point, and (iii) password access to the mobile app. The mobile app has a RESTful API and will be covered by SSL;
- (f) The Dashboard and RESTful API are secured with SSL and TLS by default;
- (g) All connections are directed through HTTPS ;
- (h) A full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*
- (i) Technical issues with the LFR system are always dealt with by member of the technical staff who support the Deployment of the LFR system.

#### 5.7 Appropriate Policy Document:

Section 42 of the DPA requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. The MPS has produced this document and published it. This document allows the public to understand details of the:

- (a) the data being processed by the LFR system, how often it is processed and whose data is processed;
- (b) procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
- (c) MPS policy for the retention and erasure of personal data for LFR processing.

#### 5.8 Data Protection Officer:

The MPS has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to LFR. The DPO is available to inform and advise the Commissioner (as data controller) and MPS personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

## 6 Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a surveillance camera code issued by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. Section 33(1) PoFA requires the MPS to have regard to the Code for the use of LFR. This includes compliance with the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which the MPS have regard to as follows:

| Code                                                       | MPS approach                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fair processing information to data subjects               | The MPS processing information publically available to data subjects. It makes information relating to the LFR and data processing available via its website. The LFR Deployments are publically disclosed with supporting information.                                                        |
| Appropriate retention and disposal systems                 | The necessary systems are addressed in the MPS LFR Documents.                                                                                                                                                                                                                                  |
| Suitable technological and physical security measures      | These measures have been addressed by design and are also covered in the MPS LFR Documents.                                                                                                                                                                                                    |
| Cameras of sufficient quality to meet the intended purpose | This requirement is addressed by the design of the LFR system.                                                                                                                                                                                                                                 |
| Monitored by trained individuals                           | The LFR system will always flag potential matches to a trained member of MPS personnel for a decision on any further action. In this way, the LFR system works to assist MPS personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input. |
| Some level of human interaction                            |                                                                                                                                                                                                                                                                                                |

The MPS has also given regard to the then Surveillance Camera Commissioner's guidance on the use of automated facial recognition technology with surveillance camera systems in order to comply with Code and its obligations under s.33 PoFA with a number of points being covered in this Legal Mandate.

## 7 Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

- (a) public authorities are obliged to publish certain information about their activities;
- (b) members of the public are entitled to request information from public authorities.

In recognition of its FOIA duties, the MPS makes significant LFR information available via its website. This includes summary information relating to LFR Deployments including the Watchlist size, the total number of Alerts, positive action and incorrect identification numbers, arrests and disposal numbers and estimates of the total number of faces seen as people passed the LFR system. The MPS will also be responsive to FOIA requests.



More Trust | Less Crime | High Standards

# MPS LFR POLICY DOCUMENT

*Direction for the MPS Deployment of  
overt Live Facial Recognition Technology to locate  
person(s) on a Watchlist*

# Table of Contents

|           |                                                                 |           |
|-----------|-----------------------------------------------------------------|-----------|
| <b>1</b>  | <b><i>Introduction, Aim and Scope .....</i></b>                 | <b>3</b>  |
| <b>2</b>  | <b><i>Document Edit History .....</i></b>                       | <b>6</b>  |
| <b>3</b>  | <b><i>Terminology .....</i></b>                                 | <b>7</b>  |
| <b>4</b>  | <b><i>LFR Overview .....</i></b>                                | <b>13</b> |
| <b>5</b>  | <b><i>Strategic Intention, Objectives and Use Case.....</i></b> | <b>15</b> |
| <b>6</b>  | <b><i>Overview of LFR Deployment Processes .....</i></b>        | <b>18</b> |
| <b>7</b>  | <b><i>Governance, Oversight and Impact Assessments.....</i></b> | <b>20</b> |
| <b>8</b>  | <b><i>Oversight Bodies and Regulatory Framework .....</i></b>   | <b>26</b> |
| <b>9</b>  | <b><i>Public Engagement .....</i></b>                           | <b>27</b> |
| <b>10</b> | <b><i>Watchlist Considerations .....</i></b>                    | <b>29</b> |
| <b>11</b> | <b><i>Guidelines for LFR .....</i></b>                          | <b>32</b> |
| <b>12</b> | <b><i>Cameras and Camera Placement .....</i></b>                | <b>33</b> |
| <b>13</b> | <b><i>Key Performance Metrics .....</i></b>                     | <b>34</b> |
| <b>14</b> | <b><i>LFR Policy Summary .....</i></b>                          | <b>35</b> |
| <b>15</b> | <b><i>Acronyms used in LFR .....</i></b>                        | <b>36</b> |
| <b>16</b> | <b><i>Government Protective Marking Scheme .....</i></b>        | <b>38</b> |

Terms & Definitions: Capitalised terms used within this LFR Policy Document shall have the meaning given to them in section 3 of this document unless otherwise defined.



# 1 Introduction, Aim and Scope

## Introduction

- 1.1 Live Facial Recognition (LFR) is used by the Metropolitan Police Service (MPS) as a precision crime-fighting tactic to locate people who are wanted by the MPS and/or the Courts. It helps us keep Londoners safe. More detail about how LFR works and how the MPS uses it can be found in section 4 (LFR Overview).
- 1.2 This MPS LFR Policy Document provides MPS personnel with direction on the overt use of LFR to locate those on a Watchlist in a legally compliant and ethical manner to enable the MPS to achieve legitimate policing aims.
- 1.3 This document specifically addresses a number of recommendations made by the London Policing Ethics Panel (LPEP) in their May 2019 report on the use of LFR. The MPS is also cognisant of the views and ongoing considerations of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner.

## Aim & Scope

- 1.4 This document aims to:-
  - a) provide MPS personnel and members of the public with information about the MPS's present strategic, operational and technology objectives for the overt use of LFR to locate those on a Watchlist, such that it enables the MPS to achieve its law enforcement purposes and is compliant with key LPEP recommendations (the Objectives); *and*
  - b) provide MPS personnel with direction on the construction of Watchlists and the Deployment of overt LFR technology by the MPS in spaces accessible to the public in order to meet the MPS's Objectives for LFR; *and*
  - c) establish the governance structure for the Deployment of LFR, ensuring that MPS use of LFR is appropriately governed and legally compliant; *and*
  - d) provide an overview of LFR technology and advise on practical issues such as camera selection and placement in order to obtain the best performance from the LFR system; *and*
  - e) as part of a published suite of documents, assist the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the MPS, as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.
- 1.5 This document relates only to the MPS's use of overt facial recognition (FR) technology to locate person(s) on a Watchlist. Facial recognition technologies have a number of potential applications within a law enforcement context. These deployment methodologies and the names adopted for each by the MPS are summarised in the table below in order to provide MPS personnel and the public with an overview of terminology, as well as to ensure precision and consistency when referring to various facial recognition technologies.

| FACIAL RECOGNITION OVERVIEW         |                            |                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                           |
|-------------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Facial Recognition – Method of use: |                            | The use of facial recognition where all people passing the system’s camera(s) are analysed by the system with results being generated at the same time as events.                                                                                                              | The use of facial recognition where:<br><br>(i) media is directly captured of a subject present; or<br><br>(ii) media is otherwise acquired in lieu of capturing it,<br><br>with the intent of subjecting it to analysis by the facial recognition system. The results of such analysis could shape events to which the footage relates in real time. | The use of facial recognition where media is analysed after the event. The result of such analysis would come sufficiently after the event such that they could not shape events to which the media related in real time. |
| Overt                               | Name                       | Live Facial Recognition (LFR)                                                                                                                                                                                                                                                  | Operator Initiated Facial Recognition (OIFR)                                                                                                                                                                                                                                                                                                          | Retrospective Facial Recognition (RFR)                                                                                                                                                                                    |
|                                     | How it may be referred to: | “... the use of overt live facial recognition to locate people on a watch list who are sought by the police ...”                                                                                                                                                               | “... the use of operator initiated facial recognition which takes an image of a particular person and uses it to either (i) help policing establish who a person in the image is or (ii) establish where a person has previously appeared in other media held by the police ...”                                                                      | “... retrospective facial recognition may be used after an event to help officers establish who a person is or whether their image matches against other media held on databases ... ”                                    |
| Covert                              | Name                       | Covert Real-Time Facial Recognition Surveillance (CRFRS)                                                                                                                                                                                                                       | Covert Operator Initiated Facial Recognition Surveillance (COIFRS)                                                                                                                                                                                                                                                                                    | RFR is not a covert capability in itself. It may however use media obtained via covert means.                                                                                                                             |
|                                     | How it may be referred to: | ... “whilst the then Surveillance Camera Commissioner has recognised a possible application for facial recognition in a covert way, subject to the Regulation of Investigatory Powers Act 2000, policing does not comment on any potential use of covert policing tactics ...” |                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                           |

- 1.6 The potential need for FR to be used covertly has been acknowledged by the then Surveillance Camera Commissioner in his December 2020 guidance, 'Facing the Camera'. The MPS is cognisant of its responsibilities under the Regulation of Investigatory Power Act 2000 (RIPA) and the training for the overt use of FR deployments includes providing the AO with assistance on

recognising where RIPA may apply when using FR. Further guidance on RIPA can also be obtained from the MPS MO5 - Covert Governance. Whilst the MPS does not confirm nor deny any covert use of FR, and the possibility is included in the summary table to help distinguish it from overt deployment methodologies, any potential covert use of FR would be beyond the scope of this document.

## **Not in Scope**

1.7 This document does **not** extend to:-

- a) manually instigated facial recognition for retrospective searching of video / still images - RFR; *or*
- b) operator initiated facial search submitted from a mobile device (or similar) in near real-time - OIFR; *or*
- c) tracking a person's movements around the country across a number of camera systems; *or*
- d) any covert use of FR systems including CRFRS and COIFRS; *or*
- e) any MPS use of third-party owned or operated FR systems, or data sharing for the purpose of facilitating the use of those systems. In such instances additional privacy considerations would be required (e.g. additional Information Sharing Agreements and audit requirements), which are beyond the scope of this document; *or*
- f) the legal framework that is applicable to the MPS's use of LFR – this is separately detailed within the MPS's Legal Mandate document.

## **Additional Documents**

1.8 A number of documents are available to supplement this document and these include the:-

- a) LFR Authorisation Process Guidance Flowchart (produced by DLS to provide legal advice for applicants and AOs);
- b) LFR Human Rights Consolidated Guidance (produced by DLS to provide legal advice for applicants and AOs);
- c) MPS LFR Standard Operating Procedure (SOP);
- d) MPS LFR Data Protection Impact Assessment (DPIA);
- e) MPS Facial Recognition Technology: Understanding accuracy and demographic differences;
- f) MPS LFR Training Document (PowerPoint).

## 2 Document Edit History

- 2.1 As a living document, this MPS LFR Policy Document will be subject to periodic review, on at least an annual basis. It is likely to be amended as the technology develops further and as the circumstances relating to LFR Deployment evolve.

| Version     | Date       | Additions/Modifications                                                                                                                                                    |
|-------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version 1.0 | 24/01/2020 | Original document.                                                                                                                                                         |
| Version 2.0 | 29/11/2021 | Updates as a part of a periodic review, incorporating points of clarification, facial recognition terminology/overview and consolidating points made elsewhere by the MPS. |
| Version 3.0 | 20/03/2023 | Updates as a part of a periodic review.                                                                                                                                    |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |
|             |            |                                                                                                                                                                            |

### 3 Terminology

- 3.1 Within the MPS and throughout the MPS LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition:

|                                |                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication                   | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents). |
| Administrator                  | means a specially trained person who has access rights to the LFR application in order to optimise and maintain its operational capability. The Administrator may also be referred to as the LFR System Engineer.                                                                                                                                                                          |
| Alert                          | means the Alert generated by the LFR system when a facial image from the video stream, which is being compared against the Watchlist, returns a comparison (similarity) score above the set Threshold.                                                                                                                                                                                     |
| Application                    | sets out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.                                                                                                                                                                                                  |
| Authorising Officer (AO)       | is the officer who provides the authorisation for LFR to be Deployed. LFR may not be used without this authorisation.                                                                                                                                                                                                                                                                      |
| Biometric Template or Template | <p>is a digital representation of the features of the face that have been extracted from the facial image.</p> <p>It is these Templates (and not the images themselves) that are used for searching. Note that Templates are proprietary to each facial recognition algorithm and new Templates will need to be generated from the original images if the algorithm is changed.</p>        |
| Blue Watchlist                 | is a Watchlist comprising of known persons that can be used to test system performance. For example, police officers / staff may be placed on a Blue Watchlist and 'seeded' into the crowd who walk through the Zone of Recognition at the start of a Deployment to measure the True Recognition Rate.                                                                                     |
| Bronze Community               | is appointed by Silver specifically to oversee and manage community engagement and issues relevant to an LFR Deployment or a series of LFR Deployments in a defined area.                                                                                                                                                                                                                  |

|                       |                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication          | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents). |
| Cancellation Report   | records details of where and when a Deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.                                                                                                                                                                                                                                         |
| Candidate Image       | means the image of a person from the Watchlist return as a result of an Alert.                                                                                                                                                                                                                                                                                                             |
| Confirmed False Alert | means, following an Engagement, it has been determined that the Engaged individual is not the same as the person in the Candidate Image in the Watchlist.                                                                                                                                                                                                                                  |
| Confirmed True Alert  | means, following an Engagement, it has been determined that the Engaged individual is the same as the person in the Candidate Image in the Watchlist.                                                                                                                                                                                                                                      |
| Deployment            | means use of an LFR system as authorised by an AO to locate those on an LFR Watchlist.                                                                                                                                                                                                                                                                                                     |
| Deployment Record     | means collectively; <ul style="list-style-type: none"> <li>• the Application (seeking approval for the LFR Deployment);</li> <li>• the Written Authority Document (provides a record of the decision making by the AO to give authorisation to deploy LFR); and</li> <li>• the Cancellation Report (recording details and results from an LFR Deployment).</li> </ul>                      |
| Engagement            | occurs when an officer communicates with a member of the public as a result of an LFR Alert. The term 'Engagement Officer' shall be construed accordingly.                                                                                                                                                                                                                                 |
| Environmental Factor  | is an external element that affects LFR system performance such as dim lighting, glare, rain, mist etc.                                                                                                                                                                                                                                                                                    |
| False Alert           | means that it is determined that the Probe Image is not the same as the Candidate Image in the Watchlist, based on Adjudication without any Engagement.                                                                                                                                                                                                                                    |
| Faces per frame       | means a configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.                                                                                                                                                                                                                                                          |

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication                                                                          | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents). |
| Facial Recognition (FR)                                                               | Is a technology which works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database generating possible matches. This is based on digital images (still or from live camera feeds).                                                                     |
| False Alert Rate<br><br>This is also known as the False Positive Identification Rate. | describes the number of individuals that are not on the Watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.                                                                                                                                                                              |
| False Negative                                                                        | Is where a person on the Watchlist passes through the Zone of Recognition but no Alert is generated. There are a number of reasons False Negatives occur, and these include System, Subject and Environmental Factors, as well as how high the Threshold is set.                                                                                                                           |
| Gold Commander                                                                        | is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment.                                                                                                                                                                                                                                                                          |
| Live Facial Recognition (LFR)                                                         | is an overt real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined Watchlist in order to locate Persons of Interest by generating an Alert when a possible match is found.                                                                                                                                           |
| LFR Engagement Officer                                                                | means an officer whose primary role is to undertake the Adjudication process following an Alert, which may or may not result in that officer undertaking an Engagement. These officers will also assist the public by answering questions and help understanding of the purpose and nature of the LFR Deployment.                                                                          |
| LFR Operator                                                                          | is the officer / member of staff operating the LFR application. They will consider Alerts, and via the Adjudication process, assist LFR Engagement Officers in deciding whether an Alert should result in further action or not.                                                                                                                                                           |
| LFR System Accuracy                                                                   | is not defined by a single figure to measure the accuracy of an LFR System – accuracy is determined by an overall assessment                                                                                                                                                                                                                                                               |

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication                     | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).                                                                                                            |
|                                  | of two metrics, the True Recognition Rate and the False Alert Rate.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MPS LFR Documents                | means the 'Level Three' MPS LFR Documents that regulate the MPS use of LFR, as more particularly identified within the MPS LFR Legal Mandate.                                                                                                                                                                                                                                                                                                                                                         |
| Primary Watchlist Category (PWC) | is the category of images on the Watchlist that directly support the primary purpose of the Deployment.                                                                                                                                                                                                                                                                                                                                                                                               |
| Probe Image                      | means the facial image submitted for a facial search against the Watchlist.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recognition Opportunity          | means the period when a person's face is visible to a LFR camera(s) as they move through the Zone of Recognition.                                                                                                                                                                                                                                                                                                                                                                                     |
| Recognition Time                 | means the average time from when a face appears in the Zone of Recognition of the camera to when the LFR system generates an Alert.                                                                                                                                                                                                                                                                                                                                                                   |
| Silver Commander                 | is the officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander.                                                                                                                                                                                                                                                                                                                                      |
| Subject Factor                   | means a factor linked to the individual. For example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.                                                                                                                                                                                                                                                                                                                               |
| System Factor                    | means a factor relating to the LFR system such as the algorithm.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Threshold                        | means the configurable point at which two images being compared will result in an Alert. The Threshold needs to be set with care to maximise the probability of returning correct suggested matches whilst keeping the number of False Alerts to an acceptable level.<br><br>(NB. It should be noted that any FR algorithm is only returning 'suggested' matches, based on the chosen Threshold, and that it is for a human to assess the true likelihood that the images relate to the same person.) |
| True Alert                       | is when it is determined that the Probe Image is the same as the Candidate Image in the Watchlist.                                                                                                                                                                                                                                                                                                                                                                                                    |



|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication                                                                             | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents).                                                                                                                                                                                                                                                                                                                    |
| True Recognition Rate<br><br>This is also known as the True Positive Identification Rate | describes the total number of times an individual(s) known to have passed through the Zone of Recognition and correctly generated an Alert, <u>as a proportion of</u> the total number of times the same individuals pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR system or not.<br><br>By way of an example, the rate would be 90% if 10 people <u>on the Watchlist</u> each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people. The same would be true if 5 people each pass the LFR system twice, and 2 Alerts were correctly generated for 4 of the people and only 1 correct Alert for the 5 <sup>th</sup> person. |
| Urgency                                                                                  | means, in the context of authorising an LFR Deployment, a Deployment that is related to an: <ul style="list-style-type: none"> <li>• Imminent threat-to-life or serious harm situation; <i>and/or</i></li> <li>• Intelligence / investigative opportunities with limited time to act, where the seriousness and potential benefits support the urgency of action.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| Watchlist                                                                                | means the set of known reference images against which a Probe Image is searched. The Watchlist is normally a subset of a much larger collection of images (for example a police force's custody image dataset) and will have been created specifically for the LFR Deployment.<br><br>The criteria for inclusion of images in a Watchlist will be determined by the intelligence, data and analysis available, as well as the policies outlined in this document.                                                                                                                                                                                                                                             |
| Written Authority Document (WAD)                                                         | provides the decision making audit trail demonstrating how the MPS LFR AO has considered the legality, necessity and proportionality of the Deployment, the safeguards that apply to the Deployment, and the alternatives that were considered but deemed to be less viable in realising the policing purpose. It also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the Deployment.                                                                                                                                                                                                                                      |
| Zone of Recognition (ZoR)                                                                | means 3-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the Zone Of Recognition is                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|              |                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjudication | means a human assessment of an Alert generated by the LFR system by an LFR Engagement Officer (supported, as needed by the LFR Operator) to decide whether to Engage further with the individual matched to a Watchlist image. In undertaking the Adjudication process, regard is to be paid to Subject, System and Environmental Factors (as further described in the MPS LFR Documents). |
|              | smaller than the field of view of the camera, e.g. not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.                                                                                                                                                                                |

## 4 LFR Overview

### LFR in a Law Enforcement Context

- 4.1 Live Facial Recognition (LFR) is used by the Metropolitan Police Service (MPS) as a precision crime-fighting tactic to locate people who are wanted by the MPS and/or the Courts. It helps us keep Londoners safe.
- 4.2 LFR helps us locate those on a Watchlist by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist of images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. Watchlist composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment.
- 4.3 LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify possible matches against persons of interest to LEAs.
- 4.4 Where the LFR system identifies a potential image match, the LFR system flags an Alert to a trained member of MPS personnel who then makes a decision as to whether any further action is required. In this way, the LFR system works to assist MPS personnel to make identifications rather than acting as an autonomous machine based process devoid of user input.

### LFR and the MPS

- 4.5 The MPS believes that LFR is a valuable precision policing tool that helps the MPS to keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.
- 4.6 The following are illustrative examples where LFR may assist the MPS with its policing purposes:-
  - a) Supporting the location and arrest of people wanted for criminal offences;
  - b) Preventing people who may cause harm from entering an area (e.g. fixated threat individuals, persons subject to football banning orders);
  - c) Supporting the location of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons deemed at risk etc.);
  - d) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.
- 4.7 Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. The MPS is conscious that the use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale

monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.

- 4.8 It is therefore incumbent on the MPS to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR.
- 4.9 In seeking to address other potential concerns, the MPS has facilitated academic research led by the University of Essex, and has proactively engaged with civil liberty interest groups, the London Policing Ethics Panel, and the London Mayor's Office (City Hall) for additional guidance. The MPS has also commissioned the National Physical Laboratory (NPL) to undertake a ground-breaking equitability study on the use of LFR technology in an operational context to further build on the high levels of diligence already conducted on the FR algorithm.
- 4.10 The MPS has listened carefully to many parties with an interest in the use of LFR and has carefully considered what safeguards are necessary to support the use of LFR. Deployments must be carefully designed and have clear documented objectives. The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality. Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any concerns the public may have about how their human rights are engaged.
- 4.11 The AO must also be satisfied that LFR Operators involved with the Deployment are appropriately trained, briefed, and accountable. Also, that equipment will be used correctly, and that those involved in the Deployment mitigate against inappropriate responses to LFR system Alerts.
- 4.12 The AO must also consider how the Deployment of LFR may impact on communities as a whole, and how the rights of everyone whose image is likely to be captured by the LFR system have been considered, and what safeguards are in place to protect them.
- 4.13 The MPS is not only concerned with developing and implementing precision policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. The MPS will implement a robust governance process to review the effectiveness and impact of LFR Deployments on an ongoing basis. The MPS will focus on delivering transparency, and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from London communities as part of an ongoing process.
- 4.14 This document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

## 5 Strategic Intention, Objectives and Use Case

- 5.1 LFR Deployments must be run under a Written Authority Document that complies with the following strategic intentions and operational objectives.

### Strategic Intentions

- 5.2 The MPS will:-

- a) use overt LFR technology in a responsible way to locate people in accordance with the MPS's common law policing powers. This includes targeting those wanted by the courts, those who pose a risk of harm and those wanted for criminal offences. The MPS will focus on its policing priorities. These include tackling serious crimes, with a particular regard to knife and gun crime, child sexual exploitation, violence against women and girls, and terrorism. The MPS will actively target the criminals, serious crime groups and those committing crimes which are regarded as having a serious impact on local communities and LFR's ability to more precisely disrupt criminality, reduce harm to the public and increase public safety; *and*
- b) strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep London safe for everyone; *and*
- c) build public trust and confidence in the development, management and use of LFR by taking account of privacy concerns and maximising transparency; *and*
- d) maintain good governance through a command structure that incorporates strategic, operational and technical leads for the Deployment of LFR, with clear decision making and accountability; *and*
- e) ensure that the Deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework (see the MPS LFR SOP and MPS LFR Legal Mandate for a schematic of this framework); *and*
- f) transparently identify, manage and mitigate reputational and organisational risk to the MPS; *and*
- g) be recognised as a responsible, exemplary and ethical organisation.

### Operational Objectives

- 5.3 The MPS will:-

- a) use LFR technology to enable the MPS to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities; *and*
- b) adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight is active and involved, with the officer retaining full control and making the decision on whether or not to take action; *and*
- c) engage with and provide reassurance to communities, listening and responding to concerns; *and*
- d) continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

## Technological Objectives

### 5.4 The MPS will:-

- a) ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; *and*
- b) provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other serious offences; *and*
- c) look to technology improvements whilst keeping the MPS model under review.

## Use Case

### 5.5 This document relates to the use of LFR in an overt capacity to locate those on a Watchlist to help the MPS protect the public. This reflects the MPS strategic intentions to place a focus on targeting criminals and serious organised crime, dismantling the organised crime groups and reducing the risk of harm facing the general public across London. From a MPS perspective, the following examples can be seen as factors that will currently inform an AO's judgment as to what constitutes 'serious crime' for the purposes of an LFR Deployment.

- 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 be reasonably be expected to have on the local community, and (iii) the threat posed to public safety.
- c) Examples where the seriousness of certain offences have 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.

### 5.6 The above factors are not exhaustive in making a determination as to what constitutes a serious crime given that all LFR Deployments are intelligence-led and reflect current MPS policing priorities and objectives. Within the parameters of the MPS LFR Documents, it remains for the AO to be satisfied that targeting people wanted for any particular crime type is lawful, necessary and proportionate in the circumstances and in line with this MPS LFR Policy.

### 5.7 The MPS will keep the use of LFR under review to ensure LFR continues to be used as an effective crime-fighting tool.

### 5.8 LFR helps the MPS use its resources more precisely and efficiently. The MPS considers that LFR is better than humans at recognising persons from a dataset and quickly linking a match, whilst providing information that indicated why they may be of interest to the MPS.

### 5.9 The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies.

### 5.10 Locations for the Deployment of LFR will be kept under strict review, with LFR being Deployed into areas where it has the greatest potential to assist the MPS in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why a

location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other MPS LFR Documents.

- 5.11 Given that LFR requires a member of MPS personnel to review every Alert in real-time for a decision as to whether any further action is required, the MPS will always deploy LFR in a way that is operationally effective and allows the MPS to act on any Alerts as they are generated. LFR will not be used indiscriminately.

## 6 Overview of LFR Deployment Processes

### End-to-End Process

- 6.1 A high level summary of end-to-end process of a stand-alone LFR Deployment can be found annexed to this MPS LFR Policy and the MPS LFR SOP. The MPS LFR SOP also provides a greater level of detail about the processes involved in the Deployment of LFR by the MPS.

### The technical operation of LFR

- 6.2 The technical operation of LFR can be summarised in six stages as follows:

| Stage | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | <b>Compiling or using an existing database of images</b><br>The LFR system requires a Watchlist of reference images, against which to compare facial images from the video feed. In order for images to be used for LFR, they are processed so that the facial features associated with their subjects are extracted and expressed as numerical values.                                                                                                                                                                                                                                                                                                                                 |
| 2     | <b>Facial image acquisition</b><br>A camera takes digital pictures of facial images in real time, capturing images as a person moves through the Zone of Recognition and using it as a live feed. The siting of the cameras, and therefore the LFR Deployment location, is important to the lawful use of LFR.                                                                                                                                                                                                                                                                                                                                                                          |
| 3     | <b>Face detection</b><br>Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 4     | <b>Feature extraction</b><br>Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5     | <b>Face comparison</b><br>The LFR software compares the biometric template with those held on the Watchlist.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 6     | <b>Matching</b><br>When the facial features from two images are compared, the LFR system generates a similarity score. This is a numerical value indicating the extent of similarity, with a higher score indicating greater points of similarity. A Threshold value is set to determine when the LFR software will generate an alert to indicate that a possible match has occurred. Trained members of police personnel will review the Alerts and make a decision as to whether any further action is required. In this way, the LFR system works to assist police personnel to make identifications, rather than acting as an autonomous machine-based process devoid of user input |



## **Key Points**

- a) LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are on a Watchlist;
- b) The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area;
- c) The quality and resolution of images (both those in the Watchlist and those from the video cameras) are of vital importance and must be carefully considered;
- d) The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.
- e) It is important to balance the objectives of the operation with the size of the Watchlist and the available resource to respond to Alerts. If the objectives are too broad and/or the Watchlist is too large, the amount of resource required to respond to Alerts may be prohibitively high.
- f) The biometric data of those who do not generate an Alert is automatically and permanently deleted.

## **Policing LFR Deployments Effectively**

- 6.3 There must be sufficient appropriately trained resource deployed so as to be able to respond to Alerts. This is important in order to ensure that the LFR system, and the data processed by it, is being effectively used.
- 6.4 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, Alert latency, and the probability of people from the Watchlist being observed by the camera (i.e occlusion) and their likely presence are all matters that must be taken into account when deciding what resources should be available.
- 6.5 It is also vital that the MPS is transparent in its use of LFR under this document. As well as using signage, the provision of sufficient policing resource will allow officers to answer questions that the public may have.

## 7 Governance, Oversight and Impact Assessments

### LPEP and MPS Stipulations

- 7.1 Following consultation with the independent London Policing Ethics Panel (LPEP), the following stipulations for the ethical deployment of LFR have been proposed and accepted by the MPS:-
- a) The overall benefits to the public must be great enough to sufficiently compensate for the potential public distrust it may invoke;
  - b) It can be evidenced that the technology itself will not result in bringing unacceptable gender or racial bias into policing operations;
  - c) Each Deployment must be appropriately assessed and authorised, demonstrating both necessity and proportionality for a specific policing purpose – the MPS Form LFR 1 provides for this process;
  - d) LFR Operators are trained to understand the risks associated with use of the software, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions;
  - e) The MPS, seeking cooperation and support from MOPAC (Mayor's Office for Policing and Crime), will develop and maintain robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency, whilst taking into account guidance from the Biometric and Surveillance Camera Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

### Governance Framework

- 7.2 MPS LFR Documents address the stipulations detailed above. Governance and operational oversight of the use of the technology is approached in three stages, as follows:-

Stage 1: Pre-Deployment;

Stage 2: Operational Deployment;

Stage 3: Post-Deployment.

### Pre-Deployment

- 7.3 Authority to Deploy LFR is an operational one, where the MPS Authorising Officer (AO) rank is set at a level of least Superintendent level. In exceptional cases of urgency, an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR.
- 7.4 Where an officer below the rank of Superintendent provides the authorisation, a Superintendent (or higher rank) must be informed as soon as practicable. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.

- 7.5 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an MPS officer of NPCC rank<sup>1</sup> (or police staff equivalent) must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-London issues are taken into account as much as possible. This affords NPCC officer (or police staff equivalent) the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.
- 7.6 A number of specific MPS documents and records need to be completed in support of each Deployment. These are set out below:-

| MPS LFR Deployment Specific Documents and Records   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pre Deployment:                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| LFR Application – MPS LFR Form 1, Part 1            | Explains how the proposed use of LFR is based on an intelligence case. The LFR application sets out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Written Authority Document – MPS LFR Form 1, Part 2 | <p>The AO's written authority provides a decision making audit trail demonstrating how the AO has considered the legality, necessity and proportionality of the Deployment of LFR, the safeguards that apply to it and the alternatives that were considered but deemed to be less viable to realise the policing purpose.</p> <p>The document will also detail and/or confirm the MPS LFR Policy / MPS LFR SOP applies in relation to:</p> <ul style="list-style-type: none"> <li>• awareness raising measures prior to and during the Deployment such that it is not covert and the public can be aware LFR is in use;</li> <li>• how fair processing information will be made available in public spaces where LFR is being deployed and on police websites;</li> <li>• how individuals can exercise their rights under data protection law;</li> <li>• the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR Deployment; and</li> <li>• the arrangements that have been made to gather metrics to assess the benefits of the deployment.</li> </ul> <p>The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.</p> |

---

<sup>1</sup> NPCC – 'NPCC rank' denotes an officer holding the rank of Commander or above.

| MPS LFR Deployment Specific Documents and Records |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assessments                                       | <p>These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Surveillance Camera Commissioner's Self-Assessment.</p> <p>These documents need to be considered by the AO when authoring a Deployment to ensure they are sufficient to address the issues arising from the proposed Deployment.</p> <p>The AO must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the Deployment is not only necessary, but also proportionate to the policing purpose.</p> <p>The Gold Commander must ensure that the assessments remain under review after the AO's authority during the pre-planning process and then during the Deployment itself.</p> <p>The MPS Data Protection Officer is an integral part of ensuring compliance with data protection legislation and the completion of the DPIA and they should continue to be engaged as necessary.</p> |
| Operational Risk Assessment                       | <p>A documented assessment of specific operational risks associated with the Deployment of LFR including decisions taken regarding mitigation. The Gold Commander is to review, amend where required and adopt the Operational Risk Assessment to ensure that it aligns with their strategic intention for the Deployment as part of the pre-Deployment process.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>During the Deployment:</b>                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Deployment Logs                                   | <p>Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Gold and Silver Commanders, and LFR Operators.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Post-Deployment:</b>                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cancellation Report – MPS LFR Form 1, Part 3.     | <p>Records details of where and when LFR was Deployed, the circumstances that brought the use of LFR to a conclusion, what resources were used, relevant statistics and performance metrics, outcomes and summary of any issues following a post-deployment review.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MPS Deployment Record                             | <p>The MPS Record of LFR Deployments includes key metrics from the Deployment that will be updated and made available to the public online.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

- 7.7 A number of other specific MPS documents that will be relevant to each MPS LFR Deployment have been completed centrally. These are set out below:-

| MPS LFR Documents and Records                                                         |                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPS Data Processing – Appropriate Policy Document                                     | MPS policy on the processing of data pursuant to the Data Protecting Act 2018 relating to LFR.                                                                                               |
| MPS Legal Mandate                                                                     | Outlines the legal considerations to be addressed in order to use LFR.                                                                                                                       |
| MPS Training Materials                                                                | Provides the necessary training to ensure those involved in authorising and deploying LFR are familiar and implement the considerations relevant to its lawful, ethical and appropriate use. |
| MPS Facial Recognition Technology: Understanding accuracy and demographic differences | Provides details on the MPS's diligence on the LFR algorithm used in terms of its statistical accuracy and demographic differential performance.                                             |

## Operational Deployment

- 7.8 Arrangements must be made to accurately record and log the dates, times and location of the Deployment.
- 7.9 The Silver Commander must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the Deployment. The Silver Commander needs to be content:-
- a) that the use of the LFR remains necessary and proportionate for the policing purposes identified in the Written Authority Document; *and*
  - b) that the safeguards identified in the written approval remain effective; *and*
  - c) that the level of officer support committed to the Deployment is enabling Alerts to be responded to effectively; *and*
  - d) that the Subject, System and Environmental Factors are such that the use of the LFR system remains effective for realising the policing purpose identified in the written approval.
- 7.10 Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples may include occlusion resulting in those sought not being presented to the camera in cases of high crowd flow, adverse weather / lighting conditions or operational events changing the resources needed in the area. The Silver Commander must be empowered and have absolute discretion to suspend or terminate the Deployment. Further details are provided within the LFR SOP.

- 7.11 In any event, the Gold Commander must conduct and record a review of the activity at suitable intervals during the Deployment. The timing and frequency of reviews is determined by the Gold Commander. A suitable period should be determined in the context of the Deployment. This review should address the continued legality, necessity and proportionality of the Deployment, as well as providing some analysis on LFR system performance and the Engagements undertaken.

## **Post-Deployment**

- 7.12 The use of LFR should be subject to debrief and review. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the Deployment.
- 7.13 Each MPS LFR Form 1 provides for an authority cancellation, once no longer required. The LFR Cancellation Report is submitted to the AO (this may be the same person as the Gold Commander) to ensure that appropriate senior oversight is maintained. Such reports should typically be produced and submitted within 31 days. These will be periodically reviewed by the SRO and the MPS FR Technology Board to consider effectiveness and trend. This ensures the outcome of LFR Deployments are subject to evaluation, which in turn should feed into oversight and scrutiny processes.
- 7.14 Post-Deployment, the MPS must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with the MPS LFR documents. This includes that:-
- a) where the LFR system does not generate an Alert that a person's biometric data is immediately automatically deleted; *and*
  - b) the data held on the encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours, following the conclusion of the Deployment.
- 7.15 Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 31 days except where:-
- a) personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*
  - b) personal data is retained in accordance with the MPS's complaints / conduct investigation policies.
- 7.16 All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-
- a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*
  - b) in accordance with the MPS's complaints / conduct investigation policies; *and/or*
  - c) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV

footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.

## 8 Oversight Bodies and Regulatory Framework

- 8.1 Within the MPS, the senior internal oversight body for LFR is the MPS FR Technology Board, which in-turn answers to the MPS Management Board. In addition, MOPAC provide oversight and scrutiny while LPEP provide independent insight and guidance.
- 8.2 The MPS LFR Legal Mandate sets out the legal framework for MPS use of LFR technology, whilst the MPS LFR Policy Document and MPS LFR SOP support implementation.
- 8.3 Further oversight opportunities arise in relation to the Information Commissioner's Office and the Biometrics and Surveillance Camera Commissioner. More detail on these roles:-

- a) Surveillance Camera Commissioner (SCC); The role of the Surveillance Camera Commissioner is to encourage compliance with the surveillance camera code of practice, review how the code is working, provide advice to ministers on whether or not the code requires amendment. On the 9<sup>th</sup> March 2021, the Home Office announced the appointment of a single Biometrics and Surveillance Camera Commissioner.

Any MPS LFR system will need to comply with this Code and the twelve guiding principles. This document seeks to apply those principles.

See [www.gov.uk/government/organisations/surveillance-camera-commissioner](http://www.gov.uk/government/organisations/surveillance-camera-commissioner);

- b) Biometrics Commissioner (BC); The Commissioner is independent of Government and aims to keep the police use and retention of biometric data under review. The Commissioner makes decisions on applications made by the police to retain DNA profiles and fingerprints, and reviews national security determinations that are made or renewed by the Police in connection with the retention of DNA profiles and fingerprints. On the 9<sup>th</sup> March 2021, the Home Office announced the appointment of a single Biometrics and Surveillance Camera Commissioner.

See: [www.gov.uk/government/organisations/biometrics-commissioner](http://www.gov.uk/government/organisations/biometrics-commissioner);

- c) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Privacy Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

See [www.gov.uk/government/organisations/information-commissioners-office](http://www.gov.uk/government/organisations/information-commissioners-office).



## 9 Public Engagement

- 9.1 Public engagement must be supported by the use of online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of Deployments. At and around the location of Deployments, notices providing information, including details of the Privacy Notice, should be distributed and feedback via e-mail should be sought.
- 9.2 Operational briefings delivered to officers and stakeholders prior to Deployments should promote openness with the public and transparency about the use of LFR. Officers should be encouraged to engage with the public to increase awareness of how LFR helps keep the public safe and how it helps bring offenders to justice. It is also helpful for officers to be in possession of information leaflets that can be handed out to the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.
- 9.3 Key stakeholders, including MOPAC, may be invited to observe the planning and Deployment of LFR.

### In Advance of Deployments

- 9.4 In advance of Deployments ensure that:-
- a) LFR Deployments are, where possible without undermining the objectives for the Deployment, prior notified to the public using MPS websites and other appropriate communication channels (including social media) – such notifications will give a purpose for the Deployment (for example, to primarily locate those wanted for violent and other serious offences and those wanted by the courts)<sup>2</sup>; *and*
  - b) LFR awareness raising measures (e.g. signs and/or leaflets) are prepared to support LFR Deployment in line with the MPS LFR SOP; *and*
  - c) literature is prepared for persons who may be Engaged (to include information outlined within a privacy notice); *and*
  - d) Officers are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a Constable in uniform to compel a person to remove anything that conceals their identity<sup>3</sup>; *and*
  - e) external engagement is considered in discussion with the MPS LFR team. It may be appropriate to pursue engagement opportunities with a number of stakeholders, including MOPAC, local authorities, and public consultative or ethical review bodies. It is

---

<sup>2</sup> Consideration should be given providing a purpose for the Deployment after the event if it was not feasible to give prior notification of the Deployment's purpose.

<sup>3</sup> The use of a section 60AA power is limited to the removal of anything that conceals a person's identity as opposed to providing specific powers in relation to the use of LFR to locate someone.

important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

## **During Deployments**

9.5 During Deployments ensure that:-

- a) awareness raising measures are used in line with the MPS LFR SOP to ensure that the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed; *and*
- b) notices with a brief explanation and reference to the MPS website are available to hand out to the public on request; *and*
- c) literature is offered to persons Engaged by officers in accordance with the policy referred to above.

## **After Deployments**

9.6 After Deployments ensure that:-

- a) information about the Deployment, including location, time, date, number of Alerts, engagements, arrests, and any other information considered helpful and suitable for disclosure, is published on the MPS website in line with the completion of the MPS LFR Form 1. Care must be taken to ensure that no personal data is published; *and*
- b) external engagement is considered in discussion with the MPS LFR team. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders, including MOPAC, local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

## 10 Watchlist Considerations

### Image Quality

- 10.1 The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. The best images are those that follow a custody or passport style image that conforms to the NPIA '*Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)*'. Further detail is included within the embedded PDF:



NPIA Standard Still  
Digital Images.pdf

- 10.2 Where multiple images of a subject are available, consideration should be given to including these in the Watchlist where it is advised that they will improve the likelihood of locating those of interest to the MPS.

### Compiling the Watchlist

- 10.3 The MPS Legal Mandate and other MPS LFR Documents provide commentary on the legal and MPS policy considerations relevant to compiling a Watchlist in a lawful way. This means that we ensure we hold the Watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes. It helps ensure the public are informed as to the grounds needed to place an image on a Watchlist, and what considerations the MPS undertake in doing so.
- 10.4 Key points include the purposes for which an image may be added to the Watchlist, ensuring the Watchlist is limited to the size needed to meet the policing purposes identified, that particular privacy considerations may attach to non-police originated images and the need to take reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. The MPS LFR SOP provides practical direction on how to follow the MPS LFR Documents, including the MPS Legal Mandate.
- 10.5 The size of the Watchlist is relevant to the level of resource that should be available to a Deployment. There must be sufficient resource available to manage the Alerts generated by the LFR system.
- 10.6 As explained in section 4 (LFR Overview), Watchlist composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment. How great that likelihood needs to be will vary between cases for inclusion, but in any case should be considered against a number of factors. This means that an AO may deem it necessary and proportionate to authorise the inclusion of people to be included in a Watchlist, even though there may not be specific intelligence to say where in London they might be found. Factors for consideration in this respect include:-
- a) Severity of 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 that they are wanted for a serious offence;

- b) Risk; The level of risk associated with an individual or the offence type sought, whether that risk is to the public or themselves;
- c) Crime trends; Where there is evidence of wider organisation, repeat offending, methodologies being replicated or numbers are exponentially rising. Emerging or specific crime issues may require a broader approach in order to reassure the public and increase community safety through the use of a precision crime-fighting tactic in order to effectively respond to crime issues.
- d) Deployment location; the specific characteristics of the Deployment location may increase the possibility or likelihood of an individual passing through as well as informing the scope and nature of the Watchlist. For example, areas around transport hubs have a lot of people transiting from place to place and other areas of London have 'pull factors' that make it likely that people from across London and beyond may frequent that area.

## **Governing the Watchlist**

- 10.7 The systems used to generate the Watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.
- 10.8 The MPS LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

## **Addressing Disproportionality**

- 10.9 In normal operational circumstances, the MPS does not create or retain a breakdown of race, gender or any other protected characteristic<sup>4</sup> of persons on a Watchlist. This mirrors the approach taken with the majority of policing tools used by the MPS.
- 10.10 The Deployment of LFR is informed by the MPS Understanding Accuracy and Bias document and driven by MPS policing priorities, intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose that determines the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, there are prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.
- 10.11 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. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a Watchlist.
- 10.12 The MPS recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. The MPS use of LFR is informed by the MPS Facial Recognition

---

<sup>4</sup> As defined in Section 4 of the Equality Act 2010.

Technology: Understanding accuracy and demographic differences document. Moreover, to ensure system functionality, regular tests are carried out using police officers and staff volunteers who are 'seeded' into a 'Blue Watchlist'. The volunteers walk through the Zone of Recognition at the start of a Deployment to measure the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated.

10.13 The MPS also carries out scientific bias testing of the LFR system when necessary – such tests, including with the NPL have been documented in the MPS Facial Recognition Technology: Understanding accuracy and demographic differences document. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.

10.14 The MPS also has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. For example, being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:-

- a) those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and Environmental Factors throughout the Deployment. Should concerns arise that the LFR system is not performing correctly, the Silver commander will halt the Deployment where necessary; *and*
- b) for the purpose of facilitating post-Deployment reviews, Alerts are retained for up to 31 days. It provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in place for the Deployment, including the reviews undertaken by the Silver and Gold Commanders during the Deployment; *and*
- c) in the event post-Deployment reviews identify an area of concern, the MPS may undertake further bias testing where this appears necessary.

## 11 Guidelines for LFR

- 11.1 A new international standard (ISO IEC 30137-1: 'Use of biometrics with video surveillance systems, Part 1: System design and specification') was published in May 2019. See [www.iso.org/standard/64935.html](http://www.iso.org/standard/64935.html).
- 11.2 ISO IEC 30137-1 provides additional detail covering technical aspects of specifying and implementing a facial recognition system for use with video cameras, including camera selection and placement, adjustment of detection and matching Thresholds, Watchlist management, and the role of the LFR Operator. It is strongly recommended that forces considering the use of LFR use the guidance to supplement the technical overview provided here. The MPS has done this.
- 11.3 MPS LFR processes and associated documentation has been developed so as to provide for a reliable means of locating individuals using LFR with high definition CCTV cameras (2MP and above). For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the LFR Operator, and associated policing resources on the ground.
- 11.4 A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this document. Directly relevant components include:-
- a) the Cameras, including cabling, and their placement; *and*
  - b) the environment in which the cameras operate; *and*
  - c) the database of reference images and associated meta data, often referred to as the Watchlist; *and*
  - d) the facial recognition software that detects faces in the footage, converts the facial images into Templates, compares these against the Watchlist and provides information on the results of the comparison (generally in the form of an Alert or a numerical score) to an LFR Operator; *and*
  - e) the LFR Operator and LFR Engagement Officer who assess Alerts and determine the appropriate course of action; *and*
  - f) having sufficient officer resource to support the Deployment.

## 12 Cameras and Camera Placement

- 12.1 Cameras must be selected so that the image resolution, frame-rate, field-of-view and low-level light performance can provide images of sufficient quality for use in the facial recognition application. Current FR systems typically require a facial image with between 50 and 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED). The FR vendor should advise on specific requirements for their system.
- 12.2 Unless the environment is well controlled, cameras must be capable of operating at Wide Dynamic Range in order to generate high quality images under a variety of lighting conditions.
- 12.3 Cameras should ideally be positioned to capture faces as close as possible to the 'face-on' condition, similar to a passport image. This typically requires the cameras to be much lower than is normally the case for existing CCTV. Camera placement and angle should be further considered where those sought may be more likely to be occluded in a busy crowd in order to maximise the prospects of location.
- 12.4 Ideally the environment should be managed such that every face is evenly illuminated. Highly directional lighting, for example strong sunlight, should be avoided, which may require consideration of how the lighting will change throughout the day.
- 12.5 In general, the Zone of Recognition will be smaller than the field of view of the camera; for example, not all faces in the field of view may be in focus and not every face in the field of view will be imaged with the minimum necessary Inter-Eye Distance (IED).
- 12.6 A typical 2MP camera will provide sufficient resolution for LFR to work on a maximum of 3 to 4 people side by side. Therefore, consideration needs to be given to camera location and the physical environment. For example, looking for opportunities to funnel or restrict the movement of people within the Zone of Recognition. However, if the flow is reduced beyond a certain level, individuals may be grouped very close together, occluding or partly occluding the faces of people (people behind people).
- 12.7 The use of an 'attractor' to direct a subject's gaze towards the camera may help to obtain better quality images.
- 12.8 Detection and processing of faces is an intensive task for a computer system. The supplier of LFR software should provide guidance on hardware requirements and the number of faces that can be simultaneously processed from within a single frame. If the system is set to process too many faces, this will potentially result in delays to the LFR system response. It may also result in missed Alerts due to 'dropped frames' where the software skips some of the video footage in an attempt to catch up.

## 13 Key Performance Metrics

- 13.1 This section covers the key performance metrics which should be gathered when deploying LFR. There are two key metrics that determine the 'accuracy' of an LFR system. These are the minimum requirements and so additional metric or indicators may well be relevant and suitable for collation and analysis (these can be specified by the AO).

### **True Recognition Rate (TRR)**

- 13.2 This is also referred to as the True Positive Identification Rate.
- 13.3 The TRR is the total number of times an individual(s) on a Watchlist known to have passed through the Zone of Recognition and correctly generate an Alert, as a proportion of the total number of times the individuals who pass through the Zone of Recognition, regardless of whether an Alert is generated by the LFR application or not.
- 13.4 This metric can only be generated by 'seeding' known subjects (for example police officers or staff) into a Blue Watchlist and measuring the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated. Users of LFR systems (and vendors) must not focus so closely on maximising this metric, as it may increase the False Alert Rate to an extent that is not possible to manage the number of false alerts.

### **False Alert Rate (FAR)**

- 13.5 This is also referred to as the False Positive Identification Rate.
- 13.6 The FAR is the number of individuals that are not on the Watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.
- 13.7 All of the TRR and FAR metrics should be recorded and reported to the SRO. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e., less than 1 in 1000) and for the MPS, this is the standard endorsed by the SRO. It should be noted that the number of false alerts generated is greatly affected by the number of subjects processed by the LFR system, and to a lesser extent, the size of the Watchlist.
- 13.8 It should be also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TRR and FAR. The Threshold needs to be set with care so as to maximise the probability of returning True alerts, whilst keeping the number of False Alerts within the 1 in 1000 levels as determined by the MPS's SRO.

### **Recognition Time (RT)**

- 13.9 A third important metric is the Recognition Time. This is the average time taken between a subject on the Watchlist passing before a camera and the generation of an alert. Note that the actual amount of time taken to act on an Alert will always be longer than the RT as additional time is needed to assess the Alert to then make a final decision on whether to Engage or not.
- 13.10 The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution video



cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

## **14 LFR Policy Summary**

- 14.1 This document relates to the operational use of LFR, and the governance and oversight regimes necessary to support Deployment.
- 14.2 It is strongly advised that officers and staff adhere to the document, as this will help ensure that the MPS use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.
- 14.3 This document will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. By exception, if a decision is contemplated which would be outside of the MPS LFR Documents, any such decisions should be supported by legal advice (this being particularly relevant given this documents are published to ensure the use of LFR is accessible and foreseeable to the public). Such decisions will be rare and would typically arise where the circumstances move beyond those contemplated by this policy and give rise to a risk to the public and/or to the police. Any such decision must be fully documented and supported by a detailed rationale. Such decisions will be cited to the LFR SRO for review. This ensures that relevant decision-making features are subject to a debrief and evaluation processes.

## 15 Acronyms used in LFR

|        |                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------|
| AFR    | Assisted Facial Recognition (also sometimes referred to as Automated Facial Recognition). See paragraph 1.5. |
| AWC    | Additional Watchlist Category                                                                                |
| AO     | Authorising Officer                                                                                          |
| BC     | Biometrics Commissioner                                                                                      |
| CCTV   | Closed Circuit Television                                                                                    |
| CFRS   | Covert Real-Time Facial Recognition Surveillance                                                             |
| CIA    | Community Impact Assessment                                                                                  |
| COIFRS | Covert Operator Initiated Facial Recognition Surveillance                                                    |
| DPA    | Data Protection Act 2018                                                                                     |
| DPIA   | Data Protection Impact Assessment                                                                            |
| EIA    | Equality Impact Assessment                                                                                   |
| FAR    | False Alert Rate                                                                                             |
| FR     | Facial Recognition                                                                                           |
| FoIA   | Freedom of Information Act                                                                                   |
| HRA    | Human Rights Act 1998                                                                                        |
| ICO    | Information Commissioner's Office                                                                            |
| IED    | Inter-Eye Distance                                                                                           |
| ISO    | International Standards Organisation                                                                         |
| LEA    | Law Enforcement Agency                                                                                       |
| LPEP   | London Policing Ethics Panel                                                                                 |
| LFR    | Live Facial Recognition                                                                                      |
| MOPAC  | Mayor's Office for Policing And Crime                                                                        |
| MOPI   | Management Of Police Information                                                                             |
| MPS    | Metropolitan Police Service                                                                                  |

|       |                                                                                                              |
|-------|--------------------------------------------------------------------------------------------------------------|
| AFR   | Assisted Facial Recognition (also sometimes referred to as Automated Facial Recognition). See paragraph 1.5. |
| NPCC  | National Police Chiefs' Council                                                                              |
| NPIA  | National Police Improvement Agency (now the College of Policing)                                             |
| NPL   | National Physical Laboratory                                                                                 |
| OIFR  | Operator-Initiated Facial Recognition                                                                        |
| PWC   | Primary Watchlist Category                                                                                   |
| RFR   | Retrospective Facial Recognition                                                                             |
| RT    | Recognition Time                                                                                             |
| SCC   | Surveillance Camera Commissioner                                                                             |
| SCCSA | Surveillance Camera Commissioner's Self-Assessment                                                           |
| SOP   | Standard Operating Procedure                                                                                 |
| SRO   | Senior Responsible Officer                                                                                   |
| TRR   | True Recognition Rate                                                                                        |
| UK    | United Kingdom                                                                                               |
| USB   | Universal Serial Bus                                                                                         |
| VSS   | Video Surveillance System                                                                                    |
| WAD   | Written Authority Document                                                                                   |
| ZoR   | Zone of Recognition                                                                                          |

## 16 Government Protective Marking Scheme

|                         |                                                                        |
|-------------------------|------------------------------------------------------------------------|
| Protective marking:     | Official                                                               |
| Publication scheme Y/N: | No                                                                     |
| Title:                  | MPS LFR Policy Document                                                |
| Version:                | Version 3.0                                                            |
| Summary:                | Guidance for the MPS Deployment of Live Facial Recognition Technology. |
| Branch:                 | MPS LFR                                                                |
| Review date:            | 20 <sup>th</sup> March 2024                                            |

---

# Police use of Facial Recognition: Factsheet

[Home Office news team](#), 29 October 2023 - [Fact sheet](#)

This factsheet provides information on police use of facial recognition technology.

## Types of facial recognition

The police use three types of facial recognition:

1. Retrospective Facial Recognition (RFR)
2. Live Facial Recognition (LFR)
3. Operator Initiated Facial Recognition (OIFR)

## Retrospective Facial Recognition

RFR is used after an event or incident as part of a criminal investigation. Images are typically supplied from CCTV, mobile phone footage, dashcam or doorbell footage or social media. These images are then compared against images of people taken on arrest to identify a suspect.

When there is a possible RFR match, a trained operator reviews the images to confirm it. An investigating officer also reviews the match to confirm accuracy.

The investigating officer will consider all of the evidence available and follow up all reasonable enquiries as in any normal investigation.

This is a key tool for the police to identify suspects more quickly and accurately. It can also help identify missing or deceased people.

A South Wales Police study found that without RFR identifications take around fourteen days, whereas with it they typically take minutes.

All police forces use the Police National Database facial search facility.

## Real life examples of how forces use this technology to catch criminals and keep people safe include:

- Craig Walters was jailed for life in 2021 after attacking a woman he followed off a bus. He was arrested within 48 hours of the incident thanks to South Wales Police using facial recognition on images captured by CCTV, including on the bus.

- Images taken by a member of the public inside a Coventry nightclub where a murder had taken place were quickly matched on the police national database to a known individual. The victim's blood was found on his clothing; he was charged and sentenced to life imprisonment.
- A two-year operation was undertaken to disrupt, deter and build intelligence of drug operations within communities in Cardiff. RFR identified those involved and generated an intelligence picture of drug dealing in the city. This led to the arrest of 69 drug dealers, with 64 being charged. 44 people are serving custodial sentences totalling 117 years.
- Multiple burglars have been caught thanks to doorbells with cameras, the modern equivalent of a thief leaving his fingerprint on a windowsill. A man was jailed for burgling the home of a vulnerable pensioner. Using RFR on a CCTV image from the pensioner's home, officers identified the suspect, arrested him the following day, and he later pleaded guilty to burglary.

## Live Facial Recognition

Live Facial Recognition (LFR) enables police to identify wanted people, a core part of policing. Every day, police officers are briefed with images of suspects to look out for. Over many years, officers have spotted individuals from these briefings and taken action to keep the public safe.

LFR does what the police have always done but much more quickly and with greater accuracy.

All deployments are targeted, intelligence-led, time-bound, and geographically limited. It lets forces place their effort where it is likely to have the greatest effect. Before a deployment, the police will inform the public where they intend to use the technology and where they can obtain more information on its use.

The technology uses live video footage of crowds passing a camera and compares their images to a specific list of people wanted by the police. The technology can precisely pick a face out of a dense crowd, something which would be impossible for an officer to do. It means the police can quickly and accurately identify wanted criminals and take them off the streets.

Following a possible LFR alert, it is always a police officer on the ground who will decide what action, if any, to take. As with normal investigations, the investigating officer must form reasonable grounds to suspect the person identified is responsible for the commission of an offence and that there is justification for an arrest. The standard procedures for investigation, evidence collection, arrest, charge, and prosecution are followed.

If the LFR system does not make a match with the watchlist, a person's biometric data is deleted immediately and automatically. The watchlist is destroyed after each operation.

It is an operational decision for individual police forces whether, how and when to use the technology, in line with the College of Police [Authorised Professional Practice](#). To date, South Wales Police (SWP), the Metropolitan Police Service (MPS) and Northamptonshire Police have used LFR.

## **Real life examples include:**

- At the Arsenal v Tottenham north London derby on 24 September 2023, it led to three arrests, including a suspected sex offender.
- A wanted sex offender was sent back to jail after being identified at the Coronation of King Charles. An image of his face matched that of a wanted suspect. He was arrested and sent back to prison for breaching the terms of his release.
- Over two busy Friday nights in Soho in August 2023 the Metropolitan Police used it to help find high harm offenders. Across the two deployments there were six accurate alerts and no false alerts. It led to the police engaging with six people, five of whom were arrested including a man wanted for possession of a bladed article and a woman wanted for breach of bail in relation to robbery.

## **Operator Initiated Facial Recognition (OIFR)**

OIFR is a mobile App that allows officers, after engaging with a person of interest, to photograph them and check their identity where they are not sure, without having to arrest them and taken them into custody.

It is at the early trial stage but has been showing positive results.

## **Frequently Asked Questions**

### **Why is the Home Office encouraging the police to make more use of facial recognition technology?**

- The Government is committed to making sure the police have the tools and technology they need to solve and prevent crimes, bring offenders to justice, and keep people safe.
- Technology such as facial recognition can help the police quickly and accurately identify those wanted for serious crimes, as well as missing or vulnerable people. It also frees up police time and resources, meaning more officers can be out on the beat, engaging with communities and carrying out complex investigations.
- The Home Office is working closely with industry and the National Police Chiefs' Council to keep pace with the rapid developments and improvements in this technology and make sure forces can use it in an effective, fair, and proportionate way.

### **Didn't the courts say that police use of live facial recognition was unlawful?**

- No. The Court of Appeal in *Bridges* in 2020 found that there is a legal framework for police to use LFR.
- However, it also found that South Wales Police did not fully comply with privacy, data protection and equality laws during two of their LFR pilots.
- Since then, the police have addressed the Court's findings:
  - The College of Policing has issued [Authorised Professional Practice](#) guidance on live facial recognition, in particular setting out the circumstances in which the police can use it, and the categories of people they can look for.
  - The National Physical Laboratory has independently tested the algorithms South Wales Police and the Metropolitan Police use, and found they were very accurate and there were no statistically significant differences in performance based on gender or ethnicity at the settings the police use.

## **What laws govern police use of facial recognition?**

- There is a comprehensive legal framework in the UK, which means that the police can only use it for a policing purpose, where necessary, proportionate, and fair.
- The police have common law powers to prevent and detect crime. At the same time, they must comply with data protection, human rights, and equalities law.
- This means that all deployments must be for a policing purpose and be necessary, proportionate, and fair.
- They need to comply with any published policies and, in the case of Live Facial Recognition, follow the College of Policing guidance.

## **What safeguards are in place to make sure facial recognition is operated fairly and without bias?**

- Its use is governed by data protection, equality, and human rights laws. It can only be used for a policing purpose, where necessary, proportionate, and fair.
- The College of Policing national guidance sets out when the police can use LFR, the categories of people they can look for, and the requirement to automatically delete the biometric data of anyone the system does not match to the watchlist.
- Following a possible LFR alert, it is always a police officer on the ground who will decide what action, if any, to take.
- When there is a possible RFR match, a trained operator reviews the images to confirm it. An investigating officer also reviews the match to confirm accuracy.
- The investigating officer will consider all of the evidence available and follow up all reasonable inquiries as in any normal investigation.
- As with normal investigations, the investigating officer must form reasonable grounds to suspect the person identified is responsible for the commission of an offence and that there is justification for an arrest.
- The standard procedures for investigation, evidence collection, arrest, charge, and prosecution are followed.
- Facial recognition technology will also never replace the need for human judgement, insight, and empathy. This is not automated decision making – police officers will always make the decisions about whether and how to use any suggested matches.



# Is it true that facial recognition is not as accurate with female or non-white faces?

- Accuracy depends on the algorithm used but is improving all the time.
- The National Physical Laboratory (NPL) tested the algorithms South Wales Police (SWP) and the Metropolitan Police Service (MPS) have been using.
- At the settings they use the NPL found that for:
  - LFR - there were no statistically significant differences in performance based on gender or ethnicity in the way they use it. In practice, at the time of publication, there have been no false alerts this year.
  - RFR and OIFR - 100% accuracy in identifying a correct match with no false matches.

## Related content

1. [National Physical Laboratory testing on facial recognition technology](#)
2. [College of Policing national guidance on live facial recognition](#)
3. [Facial recognition terminology overview](#)

**Tags:** [facial recognition software](#), [factsheet](#), [Home Office in news](#), [Home Office in the media](#), [Police](#)

---

[All GOV.UK blogs](#)   [All GOV.UK blog posts](#)   [GOV.UK](#)

[All departments](#)   [Accessibility statement](#)   [Cookies](#)

**OGI**

All content is available under the [Open Government Licence v3.0](#), except where otherwise stated

[© Crown copyright](#)



Neutral Citation Number: [2020] EWCA Civ 1058

Case No: C1/2019/2670

**IN THE COURT OF APPEAL (CIVIL DIVISION)**  
**ON APPEAL FROM THE HIGH COURT OF JUSTICE**  
**QUEEN'S BENCH DIVISION (ADMINISTRATIVE COURT)**  
**CARDIFF DISTRICT REGISTRY**  
**Haddon-Cave LJ and Swift J**  
**[2019] EWHC 2341 (Admin)**

Royal Courts of Justice  
Strand, London, WC2A 2LL

Date: 11/08/2020

**Before :**

**THE MASTER OF THE ROLLS**  
**THE PRESIDENT OF THE QUEEN'S BENCH DIVISION**  
and  
**LORD JUSTICE SINGH**

-----  
**Between :**

**R (on the application of Edward BRIDGES)**

**Appellant/  
Claimant**

**- and -**

**THE CHIEF CONSTABLE OF SOUTH WALES POLICE**

**Respondent/  
Defendant**

**- and**

**THE SECRETARY OF STATE FOR THE HOME  
DEPARTMENT**

**Interested  
Party**

**-and-**

**THE INFORMATION COMMISSIONER (1)**  
**THE SURVEILLANCE CAMERA COMMISSIONER (2)**  
**THE POLICE AND CRIME COMMISSIONER FOR  
SOUTH WALES (3)**

**Interveners**

-----  
-----

**Dan Squires QC and Aidan Wills (instructed by Liberty) for the Appellant**

**Jason Beer QC and Francesca Whitelaw** (instructed by **Special Legal Casework, South Wales Police**) for the **Respondent**  
**Richard O'Brien and Thomas Yarrow** (instructed by **the Government Legal Department**)  
for the **Interested Party**  
**Gerry Facenna QC and Eric Metcalfe** (instructed by **the Information Commissioner's Office**) for the **First Intervener**  
**Andrew Sharland QC and Stephen Kosmin** (instructed by **the Government Legal Department**) for the **Second Intervener**  
**Fiona Barton QC** (instructed by **South Wales and Gwent Police Joint Legal Services**) made  
written submissions for the **Third Intervener**

Hearing dates : 23-25 June 2020

-----  
**Approved Judgment**

**Sir Terence Etherton MR, Dame Victoria Sharp PQBD and Lord Justice Singh :**

1. This appeal concerns the lawfulness of the use of live automated facial recognition technology (“AFR”) by the South Wales Police Force (“SWP”) in an ongoing trial using a system called AFR Locate. AFR Locate involves the deployment of surveillance cameras to capture digital images of members of the public, which are then processed and compared with digital images of persons on a watchlist compiled by SWP for the purpose of the deployment. On the facts of the present case, AFR Locate has been used in an overt manner. It was not deployed as a form of covert surveillance. For that reason it is common ground that this case does not raise issues that might otherwise arise under the Regulation of Investigatory Powers Act 2000.
2. The appeal is from the order dated 4 September 2019 of Haddon-Cave LJ and Swift J in the Divisional Court of the Queen’s Bench Division dismissing the Appellant’s claim for judicial review challenging the legality of the use of AFR Locate on two particular occasions and on an ongoing basis. The grounds of challenge were that AFR is not compatible with the right to respect for private life under Article 8 of the European Convention on Human Rights (“the Convention”), which is one of the Convention rights set out in Sch.1 to the Human Rights Act 1998 (“HRA”); data protection legislation; and the Public Sector Equality Duty (“PSED”) in section 149 of the Equality Act 2010.
3. The Divisional Court recorded in its judgment the co-operative and helpful way in which the case had been presented on all sides in order to ascertain the court’s early guidance as to the legal parameters and framework relating to AFR while it is still in its trial phase and before it is rolled out nationally. This appeal has been conducted on the same basis.

**The Parties**

4. The Appellant, Edward Bridges, who was the claimant in these proceedings, is a civil liberties campaigner who lives in Cardiff. He has been supported by Liberty, the well-known independent civil liberties membership organisation. The Respondent is the Chief Constable of SWP (*Heddlu De Cymru*).
5. The Interested Party, the Secretary of State for the Home Department, is responsible for policing nationwide and has concern for the development and lawful use of technology, such as AFR, which has the potential to assist in the prevention and detection of crime. The Secretary of State has provided funding to SWP to develop AFR and in June 2018 published the Home Office Biometrics Strategy. The Secretary of State created an Oversight and Advisory Board to co-ordinate consideration of the use of facial images and AFR technology by law enforcement authorities.
6. There are two interveners who were also interveners before the Divisional Court, the Information Commissioner and the Surveillance Camera Commissioner. The Information Commissioner has specific statutory powers and responsibilities under the Data Protection Act 2018 (“the DPA 2018”), and also had responsibilities under the predecessor legislation, the Data Protection Act 1998 (“the DPA 1998”). The Surveillance Camera Commissioner is the statutory regulator of surveillance cameras. He has specific powers and responsibilities under section 34 of the Protection of Freedoms Act 2012 (“the PFA 2012”) with regard to encouraging compliance with the

Surveillance Camera Code of Practice, reviewing its operation and providing advice about the Code of Practice. His responsibilities include, in particular, regulating the use of surveillance cameras and their use in conjunction with AFR technology. In addition, this Court has received submissions (in writing only) on behalf of a third intervener, the Police and Crime Commissioner for South Wales.

### **AFR and its deployment by SWP**

7. An impressive explanation of AFR and its deployment by SWP was given in considerable detail in the judgment of the Divisional Court. For a full account, reference should be made to that judgment at [23]-[40]. There has been no criticism of the accuracy of the Divisional Court's account. We have, therefore, gratefully taken what follows from their judgment.

#### *AFR Technology*

8. AFR is a way of assessing whether two facial images depict the same person. A digital photograph of a person's face is taken and processed to extract biometric data (*i.e.* measurements of the facial features). That data is then compared with facial biometric data from images contained in a database.
9. In more detail, the technical operation of AFR comprises the following six stages:
  - (1) Compiling/using an existing database of images. AFR requires a database of existing facial images (referred to in this case as "a watchlist") against which to compare facial images and the biometrics contained in them. In order for such images to be used for AFR, they are processed so that the "facial features" associated with their subjects are extracted and expressed as numerical values.
  - (2) Facial image acquisition. A CCTV camera takes digital pictures of facial images in real time. This case is concerned with the situation where a moving image is captured when a person passes into the camera's field of view, using a live feed.
  - (3) Face detection. Once a CCTV camera used in a live context captures footage, the software (a) detects human faces and then (b) isolates individual faces.
  - (4) Feature extraction. Taking the faces identified and isolated through "face detection", the software automatically extracts unique facial features from the image of each face, the resulting biometric template being unique to that image.
  - (5) Face comparison. The AFR software compares the extracted facial features with those contained in the facial images held on the watchlist.
  - (6) Matching. When facial features from two images are compared, the AFR software generates a "similarity score". This is a numerical value indicating the likelihood that the faces match, with a higher number indicating a greater likelihood of a positive match between the two faces. A threshold value is fixed to determine when the software will indicate that a match has occurred. Fixing this value too low or too high can, respectively, create risks of a high "false alarm rate" (*i.e.* the percentage of incorrect matches identified by the software) or a high "false reject rate" (*i.e.* the percentage of true matches that are not in

fact matched by the software). The threshold value is generally suggested by the manufacturer, and depends on the intended use of the AFR system. Most AFR systems, however, allow the end user to change the threshold value to whatever they choose.

*SWP's use of AFR*

10. SWP is the police authority which is the national lead on testing and conducting trials of AFR. SWP has a licence to use proprietary AFR software developed by NEC (now North Gate Public Services (UK) Ltd) called "NeoFace Watch software".
11. SWP uses AFR in two ways. We are concerned in this appeal only with the use of the AFR system which SWP calls "AFR Locate". SWP deployed AFR Locate on about 50 occasions between May 2017 and April 2019 at a variety of large public events.
12. When AFR Locate is deployed SWP mounts CCTV cameras on police vehicles, or on poles or posts, so as to capture images of the face of anyone who passes within range of the camera. As we have described above, digital images of faces of members of the public are taken from the CCTV feeds and processed in real time to extract facial biometric information. That information is then compared with facial biometric information of persons on a watchlist prepared for the purpose of that specific deployment.
13. The watchlist is created from images held on databases maintained by SWP as part of its ordinary policing activities, primarily from a database of custody photographs held on SWP's Niche Record Management System. The images selected for inclusion on a watchlist will depend on the purpose of each specific deployment. The watchlists used in the deployments in issue in this case have included (1) persons wanted on warrants, (2) individuals who are unlawfully at large (having escaped from lawful custody), (3) persons suspected of having committed crimes, (4) persons who may be in need of protection (e.g. missing persons), (5) individuals whose presence at a particular event causes particular concern, (6) persons simply of possible interest to SWP for intelligence purposes and (7) vulnerable persons. To date, the watchlists used by SWP have comprised between 400-800 people. The maximum capacity for a watchlist is 2,000 images but, as we understand it, this is because of the limits of the technology used rather than any limitation of principle.
14. As described above, a biometric template is taken from the images on the watchlist which will then be used for the purposes of undertaking algorithmic comparisons with the facial biometrics of members of the public captured on camera.
15. If, during a deployment of AFR Locate, the software identifies a possible match between a face captured on the CCTV and an image on the watchlist, the two images are reviewed by an AFR operator ("the system operator", who is a police officer) to establish whether he or she believes that a match has in fact been made. If, upon reviewing the images of the person on the watchlist and the person whose image has been captured by CCTV, the system operator does not consider that they are the subject of interest, then no further action is taken. If, however, it is believed that there is a match, other officers stationed nearby may be notified, and they will intervene, for example by asking to speak to the person concerned and, if appropriate, using statutory powers to stop and search or arrest the person.

16. The CCTV camera records footage for the duration of any AFR Locate deployment. AFR Locate is capable of scanning 50 faces per second (although that does not necessarily mean 50 different people). Beyond those technical limitations, there is no limit on the number of persons who may have their facial biometrics captured during any given deployment. It is SWP's intention during each deployment to allow AFR Locate to process as many individuals as possible. It is clear that the numbers of persons processed are very large. Over the 50 deployments that were undertaken in 2017 and 2018, around 500,000 faces may have been scanned. The overwhelming majority of persons whose biometrics are captured and processed by SWP using AFR Locate are not suspected of any wrongdoing and are not otherwise of interest to the police.

*Data retention*

17. If no match (false or positive) is made – as in the overwhelming majority of cases – then AFR Locate does not retain the facial biometrics or image of persons whose faces are scanned. They are immediately and automatically deleted. That data is not available to the system operator or any other police officer. The CCTV feed is retained for 31 days in accordance with the standard CCTV retention period. Data associated with a match is retained within AFR Locate for up to 24 hours. In the event of no match, the data is immediately deleted.
18. SWP's Standard Operating Procedures and Data Protection Impact Assessment provide for data retention periods. These are kept under review. The current data retention periods are as follows:
  - (1) CCTV feed to AFR Locate deployments: retained for 31 days with automatic deletion as part of the "Milestone" software.
  - (2) Facial images that are not matched against: immediately deleted.
  - (3) Biometric template (regardless whether match made): immediately deleted.
  - (4) Facial images alerted against: images either deleted immediately following the deployment, or, at the latest, within 24 hours following the deployment.
  - (5) Match report to include personal information (name of individual alerted against): retained for 31 days.
  - (6) Watchlist images and related biometric template: deleted immediately following the deployment, or at the latest within 24 hours following the deployment.

*Public awareness of when AFR Locate is used*

19. When AFR is deployed, SWP take steps to inform members of the public about AFR and as to its use at the event or in the area in question. Those steps include the following: (1) prior to each AFR deployment, utilising Facebook and Twitter to advertise the deployment and its location and invite engagement with officers who are deploying the technology; (2) displaying large A2-size "Fair Processing Notices" on the AFR-equipped police vehicles on site and at approximately a 100 metre radius of the AFR cameras; and (3) handing out postcard-sized notices to members of the public in the

vicinity of each AFR deployment and to every person that is spoken to as a result of an AFR intervention. There is also material about AFR on SWP's website.

20. Whilst deployment of AFR is not covert, it is nevertheless reasonable to suppose that a large number of people whose facial biometrics are captured and processed by SWP's use of AFR are unaware of this taking place.

#### *Biometric Data*

21. The use of AFR technology involves the collection, processing and storage of a wide range of information, including (1) facial images; (2) facial features (*i.e.* biometric data); (3) metadata, including time and location, associated with the same; and (4) information as to matches with persons on a watchlist. AFR entails the processing of biometric data in the form of facial biometrics. The term "biometrics" is described in the Home Office "Biometrics Strategy – Better Public Services Maintaining Public Trust" published in June 2018 (para. 1) as "the recognition of people based on measurement and analysis of their biological characteristics or behavioural data".
22. Biometric data enables the unique identification of individuals with some accuracy. It is this which distinguishes it from many other forms of data. Facial biometrics are one of the primary forms of biometric data, alongside fingerprints and DNA.
23. Facial biometrics bear some similarity to fingerprints because both can be captured without the need for any form of intimate sampling and both concern a part of the body that is generally visible to the public. A significant difference, however, is that AFR technology enables facial biometrics to be procured without requiring the co-operation or knowledge of the subject or the use of force, and can be obtained on a mass scale.

#### *Oversight and Advisory Board*

24. The Secretary of State has set up an Oversight and Advisory Board, comprising representatives from the police, the Home Office, the Surveillance Camera Commissioner, the Information Commissioner, the Biometrics Commissioner, and the Forensic Science Regulator, to co-ordinate consideration of the use of facial imaging and AFR by law enforcement authorities.

### **The specific incidents giving rise to these proceedings**

25. In addition to challenging the lawfulness of SWP's use of AFR Locate generally, the Appellant complains about two particular occasions when AFR Locate was used in Cardiff by SWP and, he maintains, he was caught on camera. Those two occasions were: (1) on 21 December 2017 at Queen Street, a busy shopping area in Cardiff; and (2) on 27 March 2018 at the Defence Procurement, Research, Technology and Exportability Exhibition ("the Defence Exhibition") which was held at the Motorpoint Arena.

#### *21 December 2017 Deployment*

26. On 21 December 2017 SWP deployed a single marked AFR-equipped van at Queen Street in Cardiff city centre. The AFR system was live from 8:00 am to 4:00 pm. There were three watchlists for this deployment: one was of a person suspected of having committed a serious crime, another comprised 382 people wanted on warrants, and the



third comprised 536 suspects (in effect, every person suspected of committing a crime in SWP's area). There were ten possible matches during the deployment. Of these two were not true matches. In one of those cases there was no intervention. Of the eight true matches there were two arrests.

27. The Appellant says he was present at Queen Street on 21 December 2017, that he was approximately 6-10 feet from the van and that he was, accordingly, in range of the cameras. He states that he did not see signage and was given no other warning indicating that AFR was in use prior to his being in close proximity to AFR-equipped vans.

*27 March 2018 deployment*

28. On 27 March 2018 the Defence Exhibition took place at the Motorpoint Arena in Cardiff. In previous years the event had attracted disorder and persons involved in past protests had caused criminal damage and made two bomb hoax calls to disrupt the event. AFR was live between 8:30 am and 4:00 pm with the cameras focusing on the arena's entrance.
29. There were again three watchlists: one comprised subjects of interest who had been arrested at the same event the previous year, five of whom had been convicted of a variety of offences, another comprised 347 persons wanted on warrants, and the third comprised 161 suspects (linked to crimes in SWP's area ranging from summary only offences to the most serious indictable offences). No arrests were made during this deployment. There were no false alerts. There was one correct match: one of the six people who had been arrested the previous year was correctly identified as being at the event. She had made a false bomb report the previous year, and had been convicted of that offence and sentenced to a suspended sentence order of 18 months' imprisonment. The information that the offender was at the event was passed to the Event Commander, but no further action was taken.
30. The Appellant's evidence was that he attended a protest outside the Motorpoint Arena. He stated in his witness statement that he was 25-30 metres away from the AFR-equipped van, but at one point he would have been closer than that. He said that, prior to seeing the van, he was not aware that AFR was in use, and he did not observe SWP officers providing any information about the use of AFR.

**Relevant legal framework**

31. Relevant legal and other material is set out in the Annex to this judgment.

**The proceedings**

32. The claim was filed by the Appellant on 3 October 2018 and issued on 18 October 2018. It was accompanied by a detailed Statement of Facts and Grounds, in which it was stated that the Appellant challenged (1) the unlawful use of the technology against him on the two occasions mentioned above, and (2) SWP's ongoing use of AFR in public places in the police area in which he resides, giving rise to clear risk of the technology again being used against him. It was stated that the grounds for the challenge were (1) breach of Article 8 of the Convention; (2) breach of Articles 10 and 11 of the Convention; (3) breaches of data protection law, namely section 4(4) of the DPA 1998 taken with the first data protection principle in Schedule 1, section 35(1) of the DPA

2018 and section 64 of the DPA 2018; and (4) breach of the PSED. The Appellant sought declarations as to those breaches and damages.

33. In the event, ground 2 has not been pursued.
34. SWP has not challenged the Appellant's standing to bring these proceedings. It has not been possible for SWP to check either whether the Appellant's image was recorded by CCTV on 21 December 2017 or 27 March 2018 or whether his facial biometric information was processed by the AFR equipment on either occasion. For pragmatic reasons SWP has accepted the Appellant's evidence that he was present on both occasions and that on those occasions his image was recorded. SWP does not dispute that the Appellant is a victim for the purposes of section 7 of the HRA. Permission to apply for judicial review was granted by consent, SWP and the Secretary of State opposing the grounds for judicial review on the substantive merits.

### **The Divisional Court's judgment**

35. The Divisional Court heard the claim over three days. It handed down an admirably clear and comprehensive judgment on 4 September 2019. It is impossible in the following brief summary to do justice to the judgment. We do no more than summarise the principal points of the judgment in order to provide a context for this appeal and our discussion and conclusions below.

#### *Article 8 of the Convention*

36. The Divisional Court held that Article 8 was engaged. They considered that, like fingerprints and DNA, AFR technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances, and that AFR-derived biometric data is information of an intrinsically private character. They said (at [57]) that the fact that the biometric data is derived from a person's facial features that are manifest in public does not detract from that. They said (at [59]) that Article 8 is triggered by the initial gathering of the information and that it is sufficient if biometric data is captured, stored and processed, even momentarily.
37. The Divisional Court found that the interference with rights in Article 8(1) was justified by the conditions of Article 8(2). They rejected the Appellant's primary argument that the use of AFR Locate by SWP was not "in accordance with the law" for the purposes of Article 8(2) because (1) there is no legal basis for the use of AFR Locate and so SWP does not, as a matter of law, have power to deploy it, and (2) in any event, any interference with Article 8 rights is not subject to a sufficient legal framework.
38. The Divisional Court held (at [75] to [78]) that using cameras with AFR technology to obtain the biometric data of members of the public in public falls within the common law powers of the police to obtain and store information for policing purposes, and that the compilation of the watchlists is both authorised under the Police and Criminal Evidence Act 1984 and within the powers of the police at common law. This is not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy AFR Locate.

39. Having cited the general principles summarised by Lord Sumption in *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9, [2015] AC 1065 at [11] to [14] and *R (P) v Secretary of State for Justice and Another* (also known as *In re Gallagher*) [2019] UKSC 3, [2020] AC 185, at [16] to [31] applicable to the “in accordance with the law” standard for the purposes of Article 8(2), the Divisional Court held (at [84]) that there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used, comprising (in addition to the common law): (1) primary legislation, (2) secondary legislative instruments in the form of codes of practice issued under primary legislation, and (3) SWP’s own local policies.
40. As to primary legislation, the Divisional Court referred to the DPA 2018 (which they said they focused on rather than the DPA 1998 only for the sake of convenience). They said (at [85]) that it embeds key safeguards which apply to all processing of personal data, including the biometric data processed when AFR Locate is used. They referred, in particular, to the provisions in Part 3 of the DPA 2018. They observed (at [88]) that the requirements arising under the DPA 2018 are mirrored in the Code of Practice on the Management of Police Information, issued by the College of Policing under section 39A of the Police Act 1996, and that section 39A(7) of the 1996 Act requires chief police officers to have regard to that Code.
41. As to the second element of the framework, the Divisional Court said (at [91]) that they agreed with the overall submission of the Surveillance Camera Commissioner that the Surveillance Camera Code of Practice, issued by the Home Secretary pursuant to section 30 of the PFA 2012 and to which a chief officer of police must have regard, provides a full system approach to the regulation of surveillance camera systems, as it provides the legal and good practice standard which the Government expects, as well as highlighting the broader spectrum of legislative requirements which apply.
42. As to the third element of the framework, SWP’s own policies as to the use of AFR Locate, the Divisional Court said (at [92]) that the three relevant policies are (1) SWP’s Standard Operating Procedure, (2) SWP’s Deployment Reports and (3) SWP’s Policy on Sensitive Processing.
43. The Divisional Court concluded (at [96]) that, drawing everything together, the cumulative effect of (1) the provisions of the DPA, (2) the Surveillance Camera Code of Practice and (3) SWP’s own policy documents, is that the interference with the rights in Article 8(1) which is consequent on SWP’s use of AFR Locate, occurs within a legal framework that is sufficient to satisfy the “in accordance with the law” requirement in Article 8(2); and that the answer to the primary submissions of the Appellant (and the Information Commissioner who supported him on this issue) is that it is neither necessary nor practical for legislation to define the precise circumstances in which AFR Locate may be used, *e.g.* to the extent of identifying precisely which offences might justify inclusion on a watchlist as a subject of interest or precisely what the sensitivity settings should be.
44. The Divisional Court then turned to the question of whether the interference of AFR Locate with Article 8(1) satisfied the four-part proportionality test in *Bank Mellat v Her Majesty’s Treasury (No 2)* [2013] UKSC 39, [2014] AC 700. Having accepted that it was appropriate, when applying the third and fourth criteria in the context of the facts of the present case, to apply a close standard of scrutiny, the Divisional Court rejected all the substantive submissions of the Appellant on this issue. They concluded (at [101])

that the use of AFR Locate on 21 December 2017 (Queen Street) and 27 March 2018 (Motorpoint Arena) struck a fair balance and was not disproportionate. The Divisional Court further said (at 108)], regarding any future use of AFR Locate, that, on the evidence before them as to the manner in which AFR Locate was currently deployed by SWP, they were satisfied that there is no systemic “proportionality deficit” such that it can be said that future use of AFR Locate by SWP would be inevitably disproportionate.

*Data Protection claims*

45. The Divisional Court recorded (at [109]) that, although none of the deployments by SWP of AFR in issue in the proceedings took place after the commencement of the DPA 2018 (25 May 2018), all parties had requested that the legality of the deployments of AFR Locate be considered as if they had taken place after 25 May 2018 and the Divisional Court were content to do so. The Divisional Court addressed the data protection claims under three headings: (1) the claim under the DPA 1998, (2) the claim under section 35 of the DPA 2018, and (3) the claim under section 64 of the DPA 2018.
46. The primary point of dispute before the Divisional Court under the DPA 1998 was the extent to which using AFR Locate entails processing personal data, SWP contending that the only personal data processed is the data of persons on the watchlist on the ground that it is only those persons that SWP can identify by name. Having referred to the judgment of the Court of Appeal in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003, and to the decision of the CJEU in Case C-212/13 *Rynes v Urad* [2015] 1 WLR 2607, the Divisional Court concluded (at [122]) that the processing of the Appellant’s image by the AFR Locate equipment was processing his personal data because the information recorded by AFR Locate individuated him from all others, that is to say it singled him out and distinguished him from all others.
47. The Divisional Court rejected, however, the Appellant’s case that SWP acted unlawfully under section 4(4) of the DPA 1998 by failing to comply with the first data protection principle, in particular that personal data must be processed lawfully and fairly. Given their conclusion on the Appellant’s Article 8 claim, the Divisional Court were satisfied that the use of AFR Locate in December 2017 and March 2018 satisfied that condition of lawfulness and fairness.
48. Turning to the requirement in section 34 of the DPA 2018 that SWP, as a “competent authority”, had to be able to demonstrate compliance with the provisions of Chapter 2 of Part 3 of the DPA 2018 concerning law enforcement processing, the Divisional Court identified the issues in dispute as being: (1) whether (as the Appellant contended but SWP contested) the processing of the biometric data of members of the public whose faces are captured by the CCTV cameras entails “sensitive processing” as described in section 35(8) of the DPA 2018, and (2) whether (as the Appellant contended but SWP contested) AFR Locate failed to meet the requirements of section 35(5). Those requirements are that: (a) the processing is strictly necessary for a law enforcement purpose; (b) the processing meets at least one of the conditions in Schedule 8; and (c) at the time when the processing is carried out, the controller has an appropriate policy document in place. The Appellant contended that none of those requirements was satisfied.

49. On the first issue, the Divisional Court concluded (at [132] and [133]) that AFR Locate does entail sensitive processing within section 35(8) insofar as it involves processing biometric data of members of the public “for the purpose of uniquely identifying an individual” within section 35(8)(b).
50. On the second issue, the Divisional Court found that AFR Locate meets the first requirement of section 35(5). They held (at [136]) that, for all the reasons given by them in relation to proportionality in the context of Article 8, the first of the requirements at section 35(5), namely “the processing is strictly necessary for the law enforcement purpose”, was satisfied. The Divisional Court held (at [137]) that the second requirement of section 35(5), that the processing must meet at least one of the conditions in Schedule 8 to the DPA 2018, was satisfied because of compliance with paragraph 1 of Schedule 8, the processing being necessary for the reasons given by the Divisional Court in the context of proportionality and Article 8, and the relevant rule of law being the common law duty to prevent and detect crime. As to the third requirement, that the controller has an appropriate policy document in place in relation to the sensitive processing in accordance with section 42, the Divisional Court said (at [139]) that they thought it was open to question whether the policy document relied upon by SWP, entitled “Policy on Sensitive Processing for Law Enforcement Purposes” dated November 2018 (“the November 2018 Policy Document”), fully met the standard required by section 42(2). They added the following at [141]:

“For the moment, we confine ourselves to the above observations. Given the role of the Information Commissioner and the prospect of further guidance, we do not think it is necessary or desirable for this Court to interfere at the present juncture and decide whether the SWP’s current November 2018 Policy Document meets the requirements of section 42(2) of the DPA 2018. In our view, the development and specific content of that document is, for now, better left for reconsideration by the SWP in the light of further guidance from the Information Commissioner.”

51. The Divisional Court turned finally, in respect of the Appellant’s data protection claims, to his claim that SWP had failed to comply with the obligation to undertake an impact assessment complying with section 64 of the DPA 2018. The Divisional Court rejected that claim on the grounds that at all material times the processing by SWP was supported by a relevant data protection impact assessment (“DPIA”) and that, approaching the matter on the footing that SWP had brought to bear a conscientious assessment, the impact assessment prepared by SWP did meet the requirements of section 64.

*The PSED claim*

52. The Divisional Court rejected the Appellant’s claim that SWP had failed to comply with its obligation under section 149 of the Equality Act 2010 because it did not, in its assessment, consider the possibility that AFR Locate might produce results that were indirectly discriminatory on grounds of sex and/or race because it produces a higher rate of positive matches for female faces and/or for black and minority ethnic faces. The Divisional Court said (at [153]) that there was no suggestion that, as at April 2017

when the AFR Locate trial commenced, SWP either recognised or ought to have recognised that the NeoFace Watch software it had licensed might operate in a way that was indirectly discriminatory, and even at the date of the hearing there was no firm evidence that the software did produce results that suggested indirect discrimination. The Divisional Court concluded (at [158]) that the Equality Impact Assessment prepared by SWP in April 2017 demonstrated that due regard was had by SWP to the section 149(1) matters.

## **The appeal**

53. Permission to appeal has been given for all the following five grounds of appeal for which permission was sought:

Ground 1: The Divisional Court erred in concluding that the interference with the Appellant's rights under Article 8(1) of the Convention, taken with section 6 of the HRA 1998, occasioned by SWP's use of AFR on 21 December 2017 and 27 March 2018 and on an ongoing basis, was/is in accordance with the law for the purposes of Article 8(2).

Ground 2: The Divisional Court made an error of law in assessing whether SWP's use of AFR at the December 2017 and March 2018 deployments constituted a proportionate interference with Article 8 rights within Article 8(2). The Divisional Court failed to consider the cumulative interference with the Article 8 rights of all those whose facial biometrics were captured as part of those deployments.

Ground 3: The Divisional Court was wrong to hold that SWP's DPIA complied with the requirements of section 64 of the DPA 2018. The DPIA is based on two material errors of law concerning the (non)engagement of the rights in Article 8 of the Convention and the processing of the (biometric) personal data of persons whose facial biometrics are captured by AFR but who are not on police watchlists used for AFR.

Ground 4: The Divisional Court erred in declining to reach a conclusion as to whether SWP has in place an "appropriate policy document" within the meaning of section 42 of the DPA 2018 (taken with section 35(5) of the DPA 2018), which complies with the requirements of that section. Having in place such a document is a condition precedent for compliance with the first data protection principle (lawful and fair processing) contained in section 35 of the DPA 2018 where the processing of personal data constitutes "sensitive processing" within the meaning of section 35(8) of the DPA.

Ground 5: The Divisional Court was wrong to hold that SWP complied with the PSED in circumstances in which SWP's Equality Impact Assessment was obviously inadequate and was based on an error of law (failing to recognise the risk of indirect discrimination) and SWP's subsequent approach to assessing possible indirect discrimination arising from the use of AFR is flawed. It is argued that the Divisional Court failed in its reasoning to appreciate that the PSED is a continuing duty.

## Discussion

### Ground 1: Sufficient Legal Framework

54. The Divisional Court addressed what is now the subject of Ground 1 in this appeal at [79]-[97] of its judgment, where it asked the question: “Is there a sufficient legal framework for the use of AFR Locate?”
55. The Divisional Court set out the general principles on this issue at [80]:

“The general principles applicable to the ‘in accordance with the law’ standard are well-established: see generally per Lord Sumption in *Catt*, above, [11]-[14]; and in *Re Gallagher* [2019] 2 WLR 509 at [16] – [31]. In summary, the following points apply.

(1) The measure in question (a) must have ‘some basis in domestic law’ and (b) must be ‘compatible with the rule of law’, which means that it should comply with the twin requirements of ‘accessibility’ and ‘foreseeability’ (*Sunday Times v United Kingdom* (1979) 2 EHRR 245; *Sliver v United Kingdom* (1983) 5 EHRR 347; and *Malone v United Kingdom* (1984) 7 EHRR 14).

(2) The legal basis must be ‘accessible’ to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must also be ‘foreseeable’ meaning that it must be possible for a person to foresee its consequences for them and it should not ‘confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself’ (Lord Sumption in *Re Gallagher*, *ibid*, at [17]).

(3) Related to (2), the law must ‘afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise’ (*S v United Kingdom*, above, at [95] and [99]).

(4) Where the impugned measure is a discretionary power, (a) what is not required is ‘an over-rigid regime which does not contain the flexibility which is needed to avoid an unjustified interference with a fundamental right’ and (b) what is required is that ‘safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights’ (per Lord Hughes in *Beghal v Director of Public Prosecutions* [2016] AC 88 at [31] and [32]). Any exercise of power that is unrestrained by law is not ‘in accordance with the law’.

(5) The rules governing the scope and application of measures need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them (*per* Lord Sumption in *Catt* at [11]).

(6) The requirement for reasonable predictability does not mean that the law has to codify answers to every possible issue (*per* Lord Sumption in *Catt* at [11]).”

56. There was no material dispute between the parties before this Court that that was an accurate statement of the relevant principles. In applying those principles to the present context, the Divisional Court concluded as follows, at [84]:

“In our view, there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used. ... The legal framework within which AFR Locate operates comprises three elements or layers (in addition to the common law), namely: (a) primary legislation; (b) secondary legislative instruments in the form of codes of practice issued under primary legislation; and (c) SWP's own local policies. Each element provides legally enforceable standards. When these elements are considered collectively against the backdrop of the common law, the use of AFR Locate by SWP is sufficiently foreseeable and accessible for the purpose of the ‘in accordance with the law’ standard.”

57. The Divisional Court considered the legislation and policy documents and concluded as follows, at [96]-[97]:

“96. Drawing these matters together, the cumulative effect of (a) the provisions of the DPA, (b) the Surveillance Camera Code and (c) SWP's own policy documents, is that the infringement of Article 8(1) rights which is consequent on SWP's use of AFR Locate, occurs within a legal framework that is sufficient to satisfy the ‘in accordance with the law’ requirement in Article 8(2). The answer to the primary submissions of the Claimant and the Information Commissioner, is that it is neither necessary nor practical for legislation to define the precise circumstances in which AFR Locate may be used, *e.g.* to the extent of identifying precisely which offences might justify inclusion as a subject of interest or precisely what the sensitivity settings should be (*c.f.* Lord Sumption in *Catt* at [14]). Taking these matters as examples, the Data Protection Principles provide sufficient regulatory control to avoid arbitrary interferences with Article 8 rights. The legal framework that we have summarised does provide a level of certainty and foreseeability that is sufficient to satisfy the tenets of Article 8(2). It provides clear legal standards to which SWP will be held. As to the content of local policies, we take account that AFR Locate is still in a trial period. The



content of SWP's policies may be altered and improved over the course of this trial. The possibility (or even the likelihood) of such improvement is not evidence of present deficiency.

97. Finally, under this heading, we refer to the comments by the Home Secretary (in her Biometrics Strategy) as to the legal framework within which AFR Locate presently operates (see above, at paragraph 67). In our view, when considered in context, these comments should be considered as amounting to pragmatic recognition that (a) steps could, and perhaps should, be taken further to codify the relevant legal standards; and (b) the future development of AFR technology is likely to require periodic re-evaluation of the sufficiency of the legal regime. We respectfully endorse both sentiments, in particular the latter. For the reasons we have set out already, we do not consider that the legal framework is at present out of kilter; yet this will inevitably have to be a matter that is subject to periodic review in the future.”

58. We find the references by the Court to the possibility of future reconsideration of this issue a little curious. This is because either an interference is in accordance with the law or it is not. The issue of whether there is relevant “law” for this purpose is a binary question: see *In re Gallagher*, at [14] (Lord Sumption JSC). The fact that this case involved the trial of a new technology does not alter the need for any interference with Article 8 rights to be in accordance with the law.

59. Mr Squires QC invited us to have regard to hypothetical scenarios which may arise in the future, for example if the large network of CCTV cameras in this country were to be connected to AFR Locate in such a way that a person’s movements around the country could be tracked. In support of that submission Mr Squires urged upon us what was said in the dissenting judgment of Lord Kerr JSC in *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88, at [93] and [102]. In that last paragraph, Lord Kerr said that:

“A power on which there are insufficient legal constraints does not become legal simply because those who may have resort to it exercise self-restraint. It is the *potential* reach of the power rather than its actual use by which its legality must be judged.”  
(Emphasis added)

60. Apart from the fact that Lord Kerr’s was a dissenting judgment, there is always a danger of reading what a judge says in a particular case as if it were a provision of general application in a statute. 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, as Mr Squires urged us to do. 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. As Lord Bingham of Cornhill said in *Brown v Stott* [2003] 1 AC 681, at 704:

“The case law shows that the court has paid very close attention to the facts of particular cases coming before it, giving effect to factual differences and recognising differences of degree.”

61. We also accept the submission made in particular by Mr Sharland QC, on behalf of the Surveillance Camera Commissioner, that what is in issue in this appeal is the local deployment of AFR within the area of SWP. This appeal is not concerned with possible use of AFR in the future on a national basis. As Mr Sharland submits, it is well-established in the caselaw of the European Court of Human Rights that local policies can be relevant to satisfy the requirement of “in accordance with the law”. Such policies do not necessarily have to be at a national level. He cited the decision of the European Court of Human Rights in *Munjaz v United Kingdom* [2012] MHLR 351, at [83]-[95]. In that case what was in issue was the policy on seclusion of patients at a “special hospital”, Ashworth, which was a high security hospital. The European Court of Human Rights concluded that the hospital's policy of seclusion did give sufficient indication of the scope of discretion which the hospital enjoyed and that the manner of that discretion was exercised with sufficient clarity to protect the applicant against arbitrary interference with his Article 8 rights.
62. Particular reliance was placed by Mr Facenna QC, on behalf of the Information Commissioner, on the decision of the Court of Justice of the European Union in *Tele2 Sverige AB v Post-och telestyrelsen* and *R (Watson) v Secretary of State for the Home Department* (joint cases C-203/15 and C-698/15) [2017] QB 771. That case, so far as it concerned the UK, concerned the compatibility of the Data Retention and Investigatory Powers Act 2014 with EU law, including the Charter of Fundamental Rights. Article 7 of that Charter contains a guarantee which is similar to Article 8 of the Convention. The legislation empowered the Secretary of State to issue a “retention notice” on a public telecommunications operator to retain “relevant communications data” if the Secretary of State considered that the requirement was necessary and proportionate for one or more of the purposes specified in the legislation. This in effect permitted the large scale and indiscriminate retention of electronic communications data of members of the public. Although this did not include the *content* of communications, it did include much other personal data, sometimes called “metadata”: it would be possible, for example, to trace and identify the source of a communication; the date, time, duration and type of communication; and the location of mobile communications equipment (see [98]).
63. The Court of Justice laid down a series of strict and detailed conditions for the compatibility of such intrusive legislation with EU law: see [102]-[122]. For example, at [120], the Court said that what was required in that context, except in cases of urgency, was “a prior review carried out either by a court or by an independent administrative body”.
64. We consider, however, that the Court's reasoning was principally directed to the question of proportionality rather than the requirement that an interference with rights must be in accordance with the law. Secondly, it was concerned with the specific

requirements of EU law: see *e.g.* [117], which cited the specific terms of Directive 2002/58, which expressly refers to a measure having to “be subject to adequate safeguards”. Thirdly, that case concerned covert surveillance. It is common ground that the present case, in contrast, is concerned with overt surveillance.

65. Nor do we accept the Appellant’s suggested analogy with the retention of fingerprints or DNA samples, which was considered by the European Court of Human Rights in *S v United Kingdom* (2009) 48 EHRR 50. Although that case is often cited (and was cited before us) in relation to the requirement that interference with Article 8 rights must be in accordance with the law, it should be noted that the European Court of Human Rights in fact declined to answer that question: see [95]-[99] of the judgment. This was because it considered that the questions raised in that context were closely related to the broader issue of whether the interference was necessary in a democratic society and, in view of its analysis of that issue at [105]-[126], it was not necessary to decide whether the wording of section 64 of the Police and Criminal Evidence Act 1984 was compatible with the “quality of law” requirements of Article 8(2).
66. When one turns to the Court’s assessment of the proportionality issue in that case, it is clear, in our view, that its reasoning was heavily influenced by the particular sort of interference which was in issue. That case concerned the retention of fingerprints and DNA records. Furthermore, the legislation in issue permitted that retention even in the case of people such as the applicants who, having been arrested, had been acquitted and perhaps never even charged with an offence. The legislation permitted the blanket and indiscriminate retention of such personal data. There were no time limits and no restriction by reference to the type of offence. We consider, like the Divisional Court, that the context of that case is far removed from that of the present case.
67. On behalf of the Appellant Mr Squires also placed reliance on the judgment of Lord Reed JSC in *R (T) v Chief Constable of Greater Manchester and Others* [2014] UKSC 35, [2015] AC 49, at [114], where he said:
- “... in order for the interference to be ‘in accordance with the law’, there must be safeguards which have the effect of enabling the proportionality of the interference to be adequately examined. Whether the interference in a given case was in fact proportionate is a separate question.”
68. A similar point was made again by Lord Reed in *Christian Institute v Lord Advocate* [2016] UKSC 51; [2017] SC (UKSC) 29, at [80], where he cited his earlier judgment in *T*.
69. The short answer, in our view, to this submission is that the legal framework which regulates the deployment of AFR Locate *does* contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined. In particular, the regime under the DPA 2018 enables examination of the question whether there was a proper law enforcement purpose and whether the means used were strictly necessary.
70. Mr Squires also submitted, in reliance on *Christian Institute*, that it was not sufficient that it is possible for a court or tribunal to assess the question of proportionality after

the event, because a person whose Article 8 rights are interfered with may never know that the interference has taken place and should be put in a position where they are able to mount an effective challenge. It seems to us that the answer to that point is that, in the present context, as the Divisional Court found, SWP did all that could reasonably be done to bring to the public's attention that AFR Locate was being deployed at a particular place at a particular time. As is common ground, AFR Locate was deployed in an overt manner. In any event, *Christian Institute* was concerned with particular legislation of the Scottish Parliament: what was said in that case cannot be taken out of context as if it were a rule of general application set out in a statute.

71. We must now turn to the decision of the Supreme Court in *R (Catt) v Association of Chief Police Officers*. That decision formed the mainstay of the submissions for SWP and the Secretary of State, as well as the reasoning of the Divisional Court.
72. *Catt* concerned the collection, retention and use of personal data about an individual on a database whose existence was not acknowledged to exist until the judicial review proceedings in that case itself. The police maintained what was described as an "extremism database". The claimant had been a regular attendee at peace movement demonstrations since 1948. In 2005 he began participating in demonstrations of an organisation called Smash EDO, a number of which involved serious disorder and criminality. The applicant was arrested twice but never convicted of any offence. When he made a request to the police under the DPA 1998, entries on the database concerning protests at which he had taken part were disclosed to him.
73. The database contained information about the claimant in the form of a single photograph, subsequently destroyed, and written references to him in a number of information reports on other people. In the majority of those reports all that was recorded about the claimant was the fact of his presence at a protest and his date of birth and address but some also described his appearance. The police undertook the collection of the data on the basis of general common law powers.
74. The retention and use of the data were regulated by the DPA 1998, by the 2005 Code of Practice on the Management of Police Information issued by the Secretary of State pursuant to section 39A of the Police Act 1996, and by the associated administrative guidance. That framework of legal regulation was held by the Supreme Court to be sufficient. The main judgment was given by Lord Sumption JSC (with whom Lord Neuberger PSC agreed).
75. At [1], Lord Sumption began his judgment with the following:

"This appeal is concerned with the systematic *collection* and retention by police authorities of electronic data about individuals. The issue in both cases is whether the practice of the police governing retention is lawful ..." (Emphasis added)
76. We therefore reject Mr Squires's submission that *Catt* was concerned only with the retention of information and not with its collection.
77. Lord Sumption went on to note, in the same paragraph, that a particular feature of the data in that case was that they consisted entirely of records made of acts of the applicant

which took place in public. The information had not been obtained by any intrusive technique such as bugging or DNA sampling. We accept that is a feature of the present case too.

78. At [7], Lord Sumption said that, at common law, the police have the power to obtain and store information for policing purposes, *i.e.* broadly speaking for the maintenance of public order and the prevention and detection of crime. Those powers do not authorise intrusive methods of obtaining information, such as entry on private property, but they were amply sufficient to authorise the obtaining and storage of the kind of public information in that case.
79. Lord Sumption considered the question of whether the interference in that case was in accordance with the law at [11]-[17]. He concluded that it was. He rejected the suggestion that the fact that the DPA was a statute of general application meant that it did not provide sufficient protection in the specific context of data obtained or stored by the police. As Lord Sumption said at [12]:

“... It lays down principles which are germane and directly applicable to police information, and contains a framework for their enforcement on the police among others through the Information Commissioner and the courts.”
80. Lord Sumption rejected the argument advanced on behalf of the appellant in that case that he was entitled to know precisely what data would be obtained and stored or for how long. He said that that was not realistic. “The infinite variety of situations in which issues of compliance may arise and the inevitable element of judgement involved in assessing them make complete codification impossible.” (See [14] and to similar effect [11]). Lord Sumption said that what is required is law which is “reasonably predictable, if necessary with the assistance of expert advice” but, except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. “It is enough that it lays down principles which are capable of being predictably applied to any situation.”
81. For the sake of completeness, it should be noted that, when the case of *Catt* went to the European Court of Human Rights, that Court found there to be a violation of Article 8 on the ground that the interference with the applicant’s right to respect for private life was disproportionate: see *Catt v United Kingdom* (2019) 69 EHRR 7, at [128]. The Court concluded that the question of whether the interference was in accordance with the law was in that case closely related to the broader issue of whether it was necessary in a democratic society and, in view of its analysis on that question, the Court did not find it necessary to decide whether the interference was in accordance with the law: see [106]-[107].
82. Mr Beer QC urged upon us, on behalf of SWP, what he described as a “relativist approach”. He cited the judgment (in part dissenting) of Laws LJ in *R (Wood) v Metropolitan Police Commissioner* [2009] EWCA Civ 414, [2009] 4 All ER 951, at [53], where he said:

“There is some suggestion in the cases of a relativist approach, so that the more intrusive the act complained of, the more precise and specific must be the law said to justify it.”

83. In his submissions in reply Mr Squires confirmed that he would accept the “relativist” approach. We too would be prepared to accept that as a matter of principle. The crucial question, as it seems to us, is the application of that principle to the particular context.
84. We are conscious that the police have long used techniques to gather information which are undoubtedly in accordance with the law. For example, they have the power to observe what they see in a public place, to record that information and to retain it in their files. Just as the human eye can observe a person in a public place, so the police have the power to take photographs of people.
85. We do not, however, accept the submission on behalf of SWP that the present context is analogous to the taking of photographs or the use of CCTV cameras. The following features of the present case lead us to conclude that it falls somewhere in between the two poles on a spectrum which are represented by *S v UK* on the one hand and *Catt* on the other.
86. First, AFR is a novel technology.
87. Secondly, it involves the capturing of the images and processing of digital information of a large number of members of the public, in circumstances in which it is accepted that the vast majority of them will be of no interest whatsoever to the police.
88. Thirdly, it is acknowledged by all concerned that this is “sensitive” personal data, within the meaning of the DPA 2018. That Act in turn reflects EU legislation. This represents an institutional recognition of the sensitivity of the data concerned, a feature which is not present for example for ordinary photographs.
89. Fourthly, the data is processed in an automated way.
90. We accept a large part of the analysis of the Divisional Court but not all of it. We consider that the legal framework which the Divisional Court regarded as being sufficient to constitute the “law” for the purposes of Article 8(2) is on further analysis insufficient.
91. The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the “who question” at the hearing before us. The second is the “where question”. In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed.
92. The DPA 2018 and the relevant policies in substance require only that there has to be a proper law enforcement purpose. The use of the measure must then be considered to be necessary to achieve that purpose.
93. We would also emphasise that one of the elements of the system as operated in South Wales which is crucial, in our view, is that the data of anyone where there is no match

with a person on the watchlist is automatically deleted without any human observation at all and that this takes place almost instantaneously. We would hope that that feature of the current scheme would not simply be set out in a policy document by way of description but that it would be made clear that such automatic and almost instantaneous deletion is required for there to be an adequate legal framework for the use of AFR Locate.

94. We would accept, and indeed it was common ground, that it is not for the Appellant or for this Court to design a particular set of policies in order for them to comply with the quality of law requirement. We are satisfied, however, that the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law.
95. We make it clear that we would not wish to be unduly prescriptive as to the content of any new policies, for example the principle of “neither confirm nor deny” is well-established and would have to be respected.
96. It might even be that, once the “who” question can be satisfactorily resolved, that will give clear guidance as to the “where” question. This is because it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watchlist are going to be at that location.
97. We now turn in more detail to each of the three elements of the legal framework which the Divisional Court found to be sufficient to have the quality of law in the present context: the DPA 2018, the Surveillance Camera Code of Practice and SWP’s local policies.

*Data Protection Act 2018*

98. As Mr Beer pointed out at the hearing before us, the present context is governed not simply by the general provisions in the DPA 2018 but by Part 3, which deals specifically with the subject of law enforcement processing.
99. Section 31 defines “the law enforcement purposes” in this context as:

“The purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”
100. Chapter 2 of Part 3 sets out the governing principles. Section 34 provides an overview and explains that the Chapter sets out the six data protection principles. The first data protection principle, set out in section 35(1), is that processing must be lawful and fair.
101. Amongst the requirements of the first data protection principle, set out in section 35, are the following. The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is “based on law” and either (a) the data subject has given consent to the processing for that purpose or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority: see subsection (2).

102. In addition, where the processing is “sensitive processing”, it is permitted only in the two cases set out in subsections (4) and (5). Of particular relevance in the present context is subsection (5), which deals with the situation where (a) the processing is “strictly necessary” for the law enforcement purpose, (b) the processing meets at least one of the conditions in Schedule 8, and (c) at the time when the processing is carried out, the controller has an appropriate policy document in place in accordance with section 42.
103. Schedule 8, which sets out conditions for sensitive processing under Part 3, provides that the condition in paragraph 1 is met if the processing “(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest.”
104. We accept, as did the Divisional Court, that the legal protections in the DPA 2018 form an important part of the framework in determining whether the interference with the Appellant’s Article 8 rights was in accordance with the law. That Act is not, however, sufficient by itself, nor was it suggested that it is.
105. Before leaving the DPA 2018 we should mention one further matter. In the skeleton argument on behalf of the Information Commissioner it was submitted that the Divisional Court had fallen into error by putting the cart before the horse in that it had addressed the question of the requirement of law in Article 8(2) of the Convention before considering whether there had been compliance with section 35 of the DPA 2018. In particular, it was submitted that the processing of the data in the present case was not “based on law” within the meaning of section 35(2) of the DPA 2018, interpreted in accordance with the EU’s Law Enforcement Directive and the Convention, because there was no legal basis for the processing that was clear, precise and foreseeable in its application. It was also submitted that the processing was not “strictly necessary” for the law enforcement purposes as required by section 35(5)(a) of the DPA 2018.
106. Since, it was submitted, there was a breach of section 35(2), there could not be “accordance with the law” for the purpose of Article 8(2). Detailed submissions were made as to the requirements of strict necessity, citing authority from both the Court of Justice of the European Union and the Supreme Court of the UK.
107. At the hearing before us we made it clear that we did not regard these submissions as properly falling within the scope of the present appeal. The submissions were made by an intervener in the context of Ground 1 in the appeal. Ground 1 was formulated as follows on behalf of the Appellant:
- “The Divisional Court erred in concluding that the interference with the Appellant’s rights under Article 8(1) ... occasioned by the Respondent’s use of live automated facial recognition technology ... on 21 December 2017 and 27 March 2018 and on an ongoing basis was/is in accordance with the law for the purposes of Article 8(2) ECHR.”
108. It is clear therefore that the submissions advanced on behalf of the Information Commissioner, at least in writing, went beyond the scope of Ground 1 since they



focused on the requirements of domestic legislation, namely section 35 of the DPA 2018.

*The Surveillance Camera Code of Practice*

109. Section 29 of the PFA 2012 imposes a duty on the Secretary of State to prepare a Code of Practice containing guidance about surveillance camera systems. The section goes on to prescribe what the Code must contain and what it may include provision about. The term “surveillance camera systems” is defined in subsection (6) to mean:
- “(a) closed circuit television or automatic number plate recognition systems,
  - (b) any other systems for recording or viewing visual images for surveillance purposes,
  - (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or
  - (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a) (b) or (c).”
110. It was common ground that AFR falls within that definition.
111. Under section 30 of the PFA 2012 the Secretary of State must lay a draft of an order providing for the Code to come into force, and the Code itself, before Parliament. She must then make the order and issue the Code if the draft is approved by resolution of each House of Parliament. Such an order is to be in the form of a statutory instrument.
112. The effect of the Code is governed by section 33 of the PFA 2012. A relevant authority must have regard to the Code when exercising any functions to which the Code relates: see subsection (1). A relevant authority includes for this purpose any chief officer of a police force in England and Wales: see subsection (5)(j). A failure on the part of any person to act in accordance with any provision of the Code does not of itself make that person liable to criminal or civil proceedings: see subsection (2). The Code is admissible in evidence in any such proceedings: see subsection (3). In particular, a court or tribunal may take into account a failure by a relevant authority to have regard to the Code: see subsection (4).
113. Under section 34 of the PFA 2012 the Secretary of State must appoint a person as the Surveillance Camera Commissioner. The Commissioner has the following functions: (a) encouraging compliance with the Code, (b) reviewing the operation of the Code, and (c) providing advice about the Code (including changes to it or breaches of it). It is common ground that the Commissioner does not have powers of enforcement, although the Information Commissioner does.
114. The Surveillance Camera Code of Practice was issued by the Secretary of State for the Home Department in June 2013, under section 30 of the PFA 2012. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities, including for this purpose the police. It is general in its scope and

is not specifically concerned with facial recognition technology, although that topic is referred to in the Code. The Code sets out 12 guiding principles at para. 2.6. By way of example the first guiding principle is that:

“Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.”

115. Para. 3.2.3 specifically addresses the subject of facial recognition in the following way:

“Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely.”

116. Para. 4.12.1 states:

“Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.”

117. Para. 4.12.2 states:

“A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual’s details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.”

118. In the light of the fact that the Code does deal specifically with such matters, it seems to us that it could in principle also deal specifically with what the requirements are for inclusion on a police force’s watchlist. It could also deal with what policies should contain in relation to the location of the deployment of AFR Locate. As we have said earlier, the question whether such policies must be set out in a national document such as this Code or whether they should be set out in local policies determined by each police force is not a matter for this Court. It may be prudent, however, for there to be at least consistency in the content of local policies and that might be the appropriate subject of an amendment to the Code by the Secretary of State.

119. Our attention was also drawn to the guidance which has been published by the Surveillance Camera Commissioner (March 2019) on ‘The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems’.

120. The guidance does address the question of images of persons on a watchlist at paras. 14.1-14.3. We note, however, that the guidance does not contain any requirements as to the content of local police policies as to who can be put on a watchlist. Nor does it contain any guidance as to what local policies should contain as to where AFR can be deployed. Those, as we have said, are the two critical defects in the current legal framework.

*SWP's local policies*

121. As we have said, in principle a police force's local policies can constitute relevant "law" in the present context, provided they are published. The critical question, in our view, is how much discretion the policies in this case leave to the police, particularly in relation to the question who can be put on a watchlist and the question of the location where AFR Locate can be deployed.
122. When asked about these questions at the hearing Mr Beer helpfully drew our attention to a number of documents.
123. First, Mr Beer referred to the Privacy Impact Assessment produced by SWP. At para. 1.9, in addressing the question whether there is a specific business purpose that requires the use of the information, the answer included the following in relation to those on the watchlist:

"These individuals could be persons wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence is required."

124. While we can readily understand that the first three of those categories are objective, the final category is not. In effect it could cover anyone who is of interest to the police. In our judgement, that leaves too broad a discretion vested in the individual police officer to decide who should go onto the watchlist.
125. Matters are not assisted by the fact that the next document to which our attention was drawn, the DPIA produced under the DPA 2018, does not include that last category (of intelligence purposes) at all. That document (at page 5) says that the purpose of AFR is to identify and locate:
- (1) Individuals suspected of criminality and who are wanted by the courts and police.
  - (2) Individuals who may pose a risk to themselves and others.
  - (3) Individuals who may be vulnerable.
126. Mr Beer also drew our attention to what is set out in page 16 of that same document. That, however, seems to us not to be material in the present appeal, since that concerns the application of the Regulation of Investigatory Powers Act 2000. As is common ground, covert surveillance is governed by that legislation and would require authority under the system of warrants created by that Act. Overt surveillance, in contrast, such as AFR Locate (as it was carried out by SWP on the facts of the present case) does not require such authorisation.

127. Mr Beer also drew our attention to what is said at page 20 of the same document:

“Concerns have been raised by privacy experts that an individual may seek to enquire as to whether they have been included in a watchlist outside of the 24-hours retention period. Therefore, it has been deemed appropriate to be able to re-engineer watchlists. This can now be achieved via Niche RMS ‘back-end’ database by recording the nominal number of an individual extracted into a watchlist for on given date, this added functionality is available from October 2018.”

With respect, it seems to us that deals with a technical matter and does not govern the question of who can be properly placed on a watchlist.

128. Finally, in the context of who can be placed on a watchlist Mr Beer drew our attention to SWP’s Standard Operating Procedure, at page 6, where it is said:

“3. AFR Locate

The system works by means of a pre-populated **Watch List** which will contain information and images of subjects and a pre-defined response should these subjects be located by the system.

Watchlists will be both proportionate and necessary for each deployment with the rationale for inclusion detailed pre-event in the AFR Locate deployment report.

Primary factors for consideration for inclusion within a watchlist will be watchlist size, image quality, image provenance and rationale for inclusion.

The numbers of images included within a watchlist cannot exceed 2,000 due to contract restrictions but in any event 1 in 1000 false positive alert rate should not be exceeded.

Children under the age of 18 will not ordinarily feature in a watchlist due the reduced accuracy of the system when considering immature faces.

However, if there is a significant risk of harm to that individual a risk based approach will be adopted and rationale for inclusion evidenced within the deployment report.

The decision for an AFR deployment wherever possible will ultimately be made by the Silver Commander with the DSD project team acting as tactical advisors. Wherever possible the deployment of AFR Locate should be detailed with the Silver Commanders Tactical plan.

If a deployment does not feature a Silver Commander the rationale for deployment will be ratified by the Digital Services

Division Inspector and be detailed within the AFR Locate Deployment Report.”

129. Again, it seems to us, that does not govern the question of who can be put on a watchlist in the first place.
130. So far as the location of deployment is concerned, Mr Beer really was not able to draw our attention to anything which specifies where AFR Locate may be deployed. He drew our attention to the (unnumbered) paragraphs 7-9 and 11 of the Standard Operating Procedure, again at page 6 of that document. He also drew our attention to page 21 of the DPIA, where it is said:

“As we are testing the technology South Wales Police have deployed in all event types ranging from high volume music and sporting events to indoor arenas.”

That simply underlines the concern that we have in this context. First, it is a descriptive statement and does not lay down any normative requirement as to where deployment can properly take place. Secondly, the range is very broad and without apparent limits. It is not said, for example, that the location must be one at which it is thought on reasonable grounds that people on the watchlist will be present. These documents leave the question of the location simply to the discretion of individual police officers, even if they would have to be of a certain rank (a “Silver Commander”). For the above reasons this appeal will be allowed on Ground 1.

#### Ground 2: Proportionality

131. Strictly speaking, it is unnecessary for this Court to consider Ground 2 in this appeal, which relates to the question of proportionality, since, if (as we have held) the interference with the Appellant’s Article 8 rights was not in accordance with the law, one never reaches the stage of asking whether that interference was proportionate. Nevertheless, as we heard full argument on Ground 2, we will address it.
132. The Divisional Court addressed the question of proportionality at [98]-[108]. It set out the relevant principles for the objective justification of a limitation on a Convention right at [98] by setting out four questions which are now very familiar:

“If an interference with Article 8(1) rights is to be justified it must meet the four-part test in *Bank Mellat v Her Majesty’s Treasury (No 2)* [2014] AC 700, namely:

- (1) whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
- (2) whether it is rationally connected to the objective;
- (3) whether a less intrusive measure could have been used without unacceptably compromising the objective; and

(4) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

(See *per* Lord Sumption at [20]; and especially on question (3), *per* Lord Reed at [70] to [71] and [75] to [76]).”

133. As before the Divisional Court, so before this Court there is no dispute as regards the first two of those questions. Mr Squires did not make any submissions before us in relation to the third question either. What he did submit was that the Divisional Court fell into error in answering the fourth question, whether a fair balance has been struck between the rights of the individual and the interests of the community. The Court answered that question at [101] as follows:

“Nevertheless, we are satisfied that the use of AFR Locate on 21<sup>st</sup> December 2017 (Queen's Street) and 27<sup>th</sup> March 2018 (Motorpoint Arena) struck a fair balance and was not disproportionate. AFR Locate was deployed in an open and transparent way, with significant public engagement. On each occasion, it was used for a limited time, and covered a limited footprint. It was deployed for the specific and limited purpose of seeking to identify particular individuals (not including the Claimant) who may have been in the area and whose presence was of justifiable interest to the police. On the former occasion it led to two arrests. On the latter occasion it identified a person who had made a bomb threat at the very same event the previous year and who had been subject to a (suspended) custodial sentence. On neither occasion did it lead to a disproportionate interference with anybody's Article 8 rights. Nobody was wrongly arrested. Nobody complained as to their treatment (save for the Claimant on a point of principle). Any interference with the Claimant's Article 8 rights would have been very limited. The interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant's biometric data. No personal information relating to the Claimant would have been available to any police officer, or to any human agent. No data would be retained. There was no attempt to identify the Claimant. He was not spoken to by any police officer.”

134. Mr Squires accepts that, on an appeal, it is not the function of this Court simply to make its own assessment of whether an interference with a Convention right was proportionate. The question for this Court is whether the assessment made by the Divisional Court was “wrong”, bearing in mind that this appeal consists of a review rather than a re-hearing. Mr Squires submits that the Divisional Court fell into error as a matter of approach when addressing the question of proportionality. He makes two main submissions on behalf of the Appellant.

135. First, he submits that the “benefit” side of the proportionality balance needs to take into account not only the *actual* results of an operation when AFR Locate is deployed but its *anticipated* benefits. Although that may well be right as a matter of principle, it seems to us that that is a point in favour of SWP rather than the Appellant. In any event, it does not seem to us that the Divisional Court fell into error in its approach in this way.
136. Secondly, Mr Squires submits that the Divisional Court erred when examining the “cost” side of the proportionality balance by taking into account only the impact of the AFR deployment on this particular Appellant. He submits that, as a matter of common sense, account needs to be taken of the interference with the Article 8 rights not only of this particular Appellant but all other members of the public who would have been at the two venues in question when AFR Locate was deployed on 21 December 2017 and 27 March 2018.
137. In support of that submission Mr Squires cited several dicta from the Supreme Court. In particular, he referred to *R (Tigere) v Secretary of State for Business, Innovation and Skills* [2015] UKSC 57, [2015] 1 WLR 3820, at [33], [39] and [41] in the judgment of Lady Hale DPSC. For example, at [39], Lady Hale referred to “the impact on the appellant and *others in her position*” (emphasis added). Conversely, earlier in the same paragraph, as Mr Beer pointed out to us, she referred to “the fair balance to be struck between the effect on *the person* whose rights have been infringed and the interests of the community” (emphasis added).
138. Mr Squires also cited the *Christian Institute* case, at para. 90, where the Court set out the familiar criteria for assessing proportionality and, under the fourth question, summarised it as being:
- “Whether, balancing the severity of the measure’s effects on the rights of *the persons to whom it applies* against the importance of the objective, to the extent that the measure would contribute to its achievement, the former outweighs the latter (i.e. whether the impact of the rights infringement is disproportionate to the likely benefit of the impugned measure).” (Emphasis added)
139. It seems to us that the answer to a human rights question cannot depend on semantics, for example the use of the singular or the plural used by a judge in one passage in a judgment rather than in another passage. The issue has to be addressed as a matter of legal principle.
140. It may well be that in cases such as *Tigere*, where what is under challenge is a general measure, for example a policy or even a piece of legislation, it is appropriate for the Court to assess the balance between the impact on every person who is affected by the measure and the interests of the community. The present challenge, however, was not to such a general measure. The challenge was to a very specific deployment of AFR Locate on two particular occasions and the argument made in the Statement of Facts and Grounds was simply that this Appellant’s Article 8 rights had been violated.
141. It is significant that, in the Statement of Facts and Grounds, at para. 2, the complaint brought by the Appellant was formulated in the following way:

“... On at least two occasions, in December 2017 and March 2018, the Claimant was targeted by the Defendant’s use of AFR. Through this claim he challenges:

- (i) the unlawful use of this technology *against him* on both occasions, and
- (ii) the Defendant’s ongoing use of AFR in public places in the police area in which he resides, giving rise to a clear risk of the technology again being used *against him*.” (Emphasis added)

142. It is clear therefore that the substance of the complaint being made by the Appellant in this claim for judicial review was the impact of the use of AFR by SWP against him, not anyone else. This point was developed at paras. 17-22 of the Statement of Facts and Grounds, which set out more detail about the events of 21 December 2017 and 27 March 2018. The point was summarised as follows at the beginning of para. 17:

“It is the Claimant’s case that he has twice been the subject of the Defendant’s use of AFR technology ...”

143. Further, and in any event, we accept the submission made by Mr Beer on behalf of SWP that the impact on each of the other members of the public who were in an analogous situation to this Appellant on the two occasions with which we are concerned for present purposes (in December 2017 and March 2018) was as negligible as the impact on the Appellant’s Article 8 rights. An impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement.
144. For those reasons we would reject Ground 2.

Ground 3: Compliance with section 64 of the DPA 2018

145. This ground of appeal is limited to two alleged deficiencies in the DPIA. The first is that there was a material error of law “concerning the non-engagement of Article 8” of the Convention. The second is that there was a material error of law concerning “the processing of the (biometric) personal data of persons whose facial biometrics are captured by AFR but who are not on police watch lists used for AFR”.
146. Mr Squires made no oral submissions on this ground of appeal and relied upon his skeleton argument. Mr Facenna both relied on his skeleton argument and advanced oral submissions in support of this ground of appeal.
147. Three criticisms of the DPIA are made in Mr Squires’s skeleton argument. First, the DPIA’s analysis of the application of data protection principles contained no recognition that AFR entails the processing of the personal data (and still less the biometric data) of persons not on watchlists. Second, the DPIA did not acknowledge that the Article 8 rights of such persons are engaged. Third, the DPIA was silent as to the risks to other rights which are likely to be affected by the use of AFR: the rights to



freedom of assembly under Article 11 of the Convention and freedom of expression under Article 10 of the Convention. There is no further elaboration of those points. The skeleton argument concludes, on this ground of appeal, that in the light of those three alleged deficiencies, the DPIA fell foul of the test specified by the Divisional Court itself (at [146]), namely:

“If it is apparent that a data controller has approached its task on a footing that is demonstrably false, or in a manner that is clearly lacking, then the conclusion should be that there has been a failure to meet the section 64 obligation”.

148. Mr Facenna’s skeleton argument made the following criticisms of the DPIA. First, the DPIA contained no assessment of the impact of the deployment of AFR on the protection of the personal data of members of the public who might be affected by the measures. Secondly, it contained no assessment of the risks to their rights and freedoms, so that, for example, there was little or no engagement with the fact that SWP’s use of AFR involved the collection of data on a blanket and indiscriminate basis, and it placed too little weight on the interference posed by the initial collection itself and the plainly ambitious scale of the collection, particularly bearing in mind that it involved the sensitive processing of biometric data. Thirdly, the assessment did not adequately address the risk that a false positive would result in innocent members of the public having their biometric data retained for longer periods and place them at risk of being subjected to more intrusive interventions by police. Fourthly, the assessment of the right to privacy under Article 8 of the Convention, privacy risks, and possible mitigation of those risks, was negligible at best, being more concerned with the technical operation of AFR.
149. In his oral submissions Mr Facenna said that the DPIA did not contain an assessment of privacy, personal data and safeguards. He said it contained no acknowledgment that AFR involves the collection of data on a blanket and indiscriminate basis and that the risk of false positives would mean a longer period of retention. He criticised the DPIA for failing to address the potential for gender and racial bias. Generally, he submitted that there was a failure in the DPIA to provide an assessment of the risks and mitigation of them, as required by section 64 of the DPA 2018. He said that the Divisional Court’s dismissal of the claim under section 64 has to be seen in the context of the conclusion of the Divisional Court that Article 8 was not infringed for non-matched members of the public.
150. Some of the criticisms now advanced by the Appellant and the Information Commissioner in respect of the DPIA fall outside the alleged two material errors of law specified in this ground of appeal. They include the point in Mr Squires’s skeleton argument that the DPIA does not refer to interference with the Convention rights to freedom of assembly and expression (Articles 10 and 11) and Mr Facenna’s arguments that a false positive would result in innocent members of the public having their biometric data retained for longer periods and place them at risk of being subjected to more intrusive interventions by police and that the DPIA failed to address the potential for gender and racial bias.
151. We agree with the Divisional Court that some of the criticisms of the DPIA made by Mr Squires and Mr Facenna are unjustified. The DPIA specifically acknowledged that

AFR might be perceived as being privacy intrusive in the use of biometrics and facial recognition and that Article 8 of the Convention was relevant. It sought to explain that AFR would only avoid being in breach of Article 8 if it was necessary, proportionate, in pursuit of a legitimate aim and in accordance with the law but that all those requirements would be satisfied if AFR Locate was used in the manner set out. The DPIA explained how AFR Locate operates. It is obvious from that explanation that large numbers of the public would be caught through CCTV cameras used in the deployment. It specifically stated that: “It is the intention during each deployment to allow the AFR application to enrol and therefore process as many individuals as possible”. That the public at large was potentially affected was reflected in the statement that: “in order to ensure that the public are engaged in the use of the technology every opportunity has been taken to demonstrate its use, to include during Automated Facial Recognition deployments”.

152. This Ground of Appeal is, however, correct insofar as it states that the DPIA proceeds on the basis that Article 8 is not engaged or, more accurately, is not infringed. We have found, when considering Ground 1 above, that AFR Locate fails to satisfy the requirements of Article 8(2), and in particular the “in accordance with the law” requirement, because it involves two impermissibly wide areas of discretion: the selection of those on watchlists, especially the “persons where intelligence is required” category, and the locations where AFR may be deployed.
153. The inevitable consequence of those deficiencies is that, notwithstanding the attempt of the DPIA to grapple with the Article 8 issues, the DPIA failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found, as required by section 64(3)(b) and (c) of the DPA 2018.
154. For those reasons, we will allow the appeal on this ground.

#### Ground 4: Compliance with section 42 of the DPA 2018

155. The Appellant submits that one of the reasons why the use of AFR involves the unlawful processing of personal data is because SWP has failed to satisfy the requirements of the first data protection principle in section 35 of the DPA 2018. The Divisional Court held that the processing was for law enforcement purposes and was sensitive processing within section 35(3). In the circumstances of the present case, this meant that the processing had to satisfy the requirements in section 35(5), which included (in section 35(5)(c)) that, “at the time when the processing is carried out, the controller has an appropriate policy document in place”. Section 42 of the DPA 2018 sets out what such a document must contain.
156. As stated earlier, before the Divisional Court SWP relied on the November 2018 Policy Document. The Divisional Court thought that it was open to question whether that document, as then drafted, fully met the standard required by section 42(2) and said that ideally it should be more detailed. In paragraph [141] of their judgment, which we have quoted in full above, the Divisional Court said that the development and specific content of the document was, for the time being, better left for reconsideration by SWP in the light of further guidance from the Information Commissioner.

157. The Appellant's criticism is that the Divisional Court was obliged to reach a finding on whether the November 2018 Policy Document complied with section 42, and ought to have found that it did not.
158. We would reject this ground of appeal for reasons which can be shortly stated.
159. The two specific deployments which are the subject of the Appellant's claim took place on 21 December 2017 (Queen Street) and 27 March 2018 (Motorpoint Arena). Those were before the DPA 2018 came into force. There is no alleged failure to comply with the DPA 1998 on this point.
160. Accordingly, the only relevance of compliance with section 42 was in relation to any future use of AFR in which the Appellant's image might be captured and processed by AFR. A section 42 document is an evolving document, which, in accordance with section 42(3), must be kept under review and updated from time to time. At the time of the hearing before the Divisional Court no guidance had been issued by the Information Commissioner as to the contents of a section 42 document. The Divisional Court said (at [140]) that it would be desirable to see specific guidance from the Information Commissioner, in exercise of her powers under Schedule 13 to the DPA 2018, on what is required to meet the section 42 obligation. The Information Commissioner herself expressed the view to the Divisional Court that the November 2018 Policy Document contained sufficient information to comply with the requirements of section 42(2), if barely so. That view has been repeated by the Information Commissioner on this appeal. In the event, on 4 November 2019, after the Divisional Court's judgment, the Information Commissioner did publish guidance on what a section 42 document should contain – "Law Enforcement Processing: Part 3 Appropriate Policy Document Template". SWP have now revised their November 2018 Policy Document in the light of that guidance.
161. In those circumstances - particularly as the Information Commissioner had expressed the view to the Divisional Court that the November 2018 Policy Document satisfied section 42(2) but ideally should be more detailed and the Divisional Court itself was uncertain whether or not it did meet the standard required by section 42 - it was entirely appropriate for the Divisional Court to make no final judgment on the point and to leave the SWP to make such revisions as might be appropriate in the light of any future guidance by the Information Commissioner.
162. For those reasons we would reject this ground of appeal.

Ground 5: Public Sector Equality Duty

163. The terms of the PSED are set out in section 149(1) of the Equality Act 2010 as follows:
- "A public authority must, in the exercise of its functions, have due regard to the need to—
- (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;

- (b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
- (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.”

164. The two protected characteristics that are relevant in the present case are race and sex. It is submitted on behalf of the Appellant that SWP are in breach of the PSED because they have never had due regard to the need to eliminate discrimination on those two grounds which may arise from the software which is used in the deployment of AFR Locate. It is said that there is scientific evidence that facial recognition software can be biased and create a greater risk of false identifications in the case of people from black, Asian and other minority ethnic (“BAME”) backgrounds, and also in the case of women.
165. It is important to be clear that it is not alleged that the software used by SWP does have that effect. There is no claim brought on the basis of the negative obligations in the Equality Act, not to discriminate (whether directly or indirectly). Rather the complaint is based on an alleged breach of the positive duty to have due regard to the need to eliminate such discrimination.
166. As we have mentioned above, Ground 5 in this appeal was formulated as follows:
- “The Divisional Court was wrong to hold that the Respondent complied with the Public Sector Equality Duty in section 149 of the Equality Act 2010 in circumstances in which the Respondent’s Equality Impact Assessment was obviously inadequate and based on an error of law (by failing to recognise the risk of indirect discrimination) and the Respondent’s subsequent approach to assessing possible indirect discrimination arising from the use of AFR is flawed.”
167. In the Appellant’s skeleton argument for this appeal, at para. 47, the submission was maintained that the Equality Impact Assessment dated 13 April 2017 was erroneous in law because consideration was given only to the possibility that AFR might be *directly* discriminatory and no consideration was given to whether it might operate in an *indirectly* discriminatory manner. This argument was not pursued by Mr Squires at the hearing before us, although he did not formally abandon it. He made clear during the course of the hearing, when pressed by the Court, that his focus was on the alleged *continuing* failure to discharge the PSED, and not upon the Equality Impact Assessment of April 2017.
168. The Equality Impact Assessment of April 2017 was headed “Initial Assessment”. The use of the word “initial” did not mean that the assessment was only provisional or that there would be a further or fuller assessment in due course. It meant only that the initial assessment had not led to any concerns which were thought to require further investigation. In any event, as is common ground, there has been no further Equality

Impact Assessment since April 2017. The focus of Mr Squires's submissions before us was on the point that the PSED is a continuing duty and, submits Mr Squires, there is a continuing breach of it.

169. This has always been part of the Appellant's case: see para. 92 of the Statement of Facts and Grounds, where it was made clear that the PSED is "an ongoing obligation."
170. The reasons of the Divisional Court for rejecting this ground of challenge were set out at [153]-[158] of its judgment.
171. At [153] the Divisional Court said:

"In our view, on the facts of this case there is an air of unreality about the Claimant's contention. There is no suggestion that as at April 2017 when the AFR Locate trial commenced, SWP either recognised or ought to have recognised that the software it had licensed might operate in a way that was indirectly discriminatory. Indeed, even now there is no firm evidence that the software does produce results that suggest indirect discrimination. Rather, the Claimant's case rests on what is said by Dr Anil Jain, an expert witness. In his first statement dated 30<sup>th</sup> September 2018, Dr Jain commented to the effect that the accuracy of AFR systems generally could depend on the dataset used to 'train' the system. He did not, however, make any specific comment about the dataset used by SWP or about the accuracy of the NeoFace Watch software that SWP has licensed. Dr Jain went no further than to say that if SWP did not know the contents of the dataset used to train its system 'it would be difficult for SWP to confirm whether the technology is in fact biased'. The opposite is, of course, also true."

172. At [156]-[158] the Divisional Court said the following:

"156. Thus, SWP may now, in light of the investigation undertaken to date by Mr. Edgell, wish to consider whether further investigation should be done into whether the NeoFace Watch software may produce discriminatory impacts. When deciding whether or not this is necessary it will be appropriate for SWP to take account that whenever AFR Locate is used there is an important failsafe: no step is taken against any member of the public unless an officer (the systems operator) has reviewed the potential match generated by the software and reached his own opinion that there is a match between the member of the public and the watchlist face.

157. Yet this possibility of future action does not make good the argument that to date, SWP has failed to comply with the duty under section 149(1) of the Equality Act 2010. Our conclusion is that SWP did have the due regard required when in April 2017 it commenced the trial of AFR Locate. At that time,

there was no specific reason why it ought to have been assumed it was possible that the NeoFace Watch software produced more or less reliable results depending on whether the face was male or female, or white or minority ethnic. As we have explained, even now there is no particular reason to make any such assumption. We note that although Dr Jain states that ‘bias has been found to be a feature of common AFR systems’ he does not provide an opinion on whether, or the extent to which, such bias can be addressed by the fail-safe, such as ensuring that a human operator checks whether there is in fact a match.

158. In our view, the April 2017 Equality Impact Assessment document demonstrates that due regard was had by SWP to the section 149(1) criteria. The Claimant's contention that SWP did not go far enough in that it did not seek to equip itself with information on possible or potential disparate impacts, based on the information reasonably available at that time, is mere speculation. In any event, as matters had developed in the course of the trial since April 2017, it is apparent from Mr. Edgell's evidence that SWP continues to review events against the section 149(1) criteria. This is the approach required by the public-sector equality duty in the context of a trial process. For these reasons, the claim made by reference to section 149(1) of the Equality Act 2010 fails.”

173. With respect to the Divisional Court, we do not consider that there is “an air of unreality” about the Appellant’s contention that there has been a breach of the PSED. On the contrary, it seems to us to raise a serious issue of public concern, which ought to be considered properly by SWP.
174. The Divisional Court did not refer to any authority on the PSED, perhaps because the relevant legal principles were not in dispute. In any event, those principles were set out by McCombe LJ in *R (Bracking) v Secretary of State for Work and Pensions* [2013] EWCA Civ 1345, [2014] Eq LR 60, at [26]. It is unnecessary to set out that passage in full here. It is well known and has frequently been cited with approval since, including in *Hotak v Southwark LBC* [2015] UKSC 30, [2016] AC 811, at [73] (Lord Neuberger PSC).
175. In that summary McCombe LJ referred to earlier important decisions, including those of the Divisional Court in *R (Brown) v Secretary of State for Work and Pensions* [2008] EWHC 3158 (Admin); [2009] PTSR 1506, in which the judgment was given by Aikens LJ; and *R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills* [2012] EWHC 201 (Admin); [2012] HRLR 13, in which the judgment was given by Elias LJ. For present purposes we would emphasise the following principles, which were set out in McCombe LJ’s summary in *Bracking* and are supported by the earlier authorities:

(1) The PSED must be fulfilled before and at the time when a particular policy is being considered.

- (2) The duty must be exercised in substance, with rigour, and with an open mind. It is not a question of ticking boxes.
  - (3) The duty is non-delegable.
  - (4) The duty is a continuing one.
  - (5) If the relevant material is not available, there will be a duty to acquire it and this will frequently mean that some further consultation with appropriate groups is required.
  - (6) Provided the court is satisfied that there has been a rigorous consideration of the duty, so that there is a proper appreciation of the potential impact of the decision on equality objectives and the desirability of promoting them, then it is for the decision-maker to decide how much weight should be given to the various factors informing the decision.
176. We accept (as is common ground) that the PSED is a duty of process and not outcome. That does not, however, diminish its importance. Public law is often concerned with the process by which a decision is taken and not with the substance of that decision. This is for at least two reasons. First, good processes are more likely to lead to better informed, and therefore better, decisions. Secondly, whatever the outcome, good processes help to make public authorities accountable to the public. We would add, in the particular context of the PSED, that the duty helps to reassure members of the public, whatever their race or sex, that their interests have been properly taken into account before policies are formulated or brought into effect.
177. This is reinforced by the background to the enactment of the PSED. That background is to be found in the Stephen Lawrence Inquiry Report in 1999, which led to the Race Relations (Amendment) Act 2000. That Act introduced a new section 71 into the Race Relations Act 1976, to replace an earlier version which had applied only to local authorities. The provision has since been expanded to embrace other protected characteristics and now finds its place in section 149 of the Equality Act 2010.
178. The background is explained by Karon Monaghan QC in Equality Law (2<sup>nd</sup> ed., 2013), at para. 16.06:
- “The first of the modern equality duties was found again in section 71 of the RRA, but following amendments made to it by the Race Relations (Amendment) Act 2000 (enacting the General Race Equality Duty). The General Race Equality Duty in the amended section 71 of the RRA required that listed public authorities had ‘due regard’ to the need ‘to eliminate unlawful racial discrimination’ and ‘to promote equality of opportunity and good relations between persons of different racial groups’. The Race Relations (Amendment) Act 2000 and the General Race Equality Duty within it were enacted to give effect to the recommendations in the Stephen Lawrence Inquiry Report and the Inquiry’s findings of ‘institutional racism’. The purpose of the General Race Equality Duty was to create a strong, effective,

and enforceable legal obligation which placed race equality at the heart of the public authority's decision making. The new duty was intended to mark a major change in the law. It represented a move from a fault-based scheme where legal liability rested only with those who could be shown to have committed one or other of the unlawful acts. Instead, the duty-bearer, the public authority, was to be required to *proactively* consider altering its practices and structures to meet this statutory duty. This was considered important in light of the findings of the Stephen Lawrence Inquiry.” (Emphasis added)

179. Public concern about the relationship between the police and BAME communities has not diminished in the years since the Stephen Lawrence Inquiry Report. The reason why the PSED is so important is that it requires a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population.
180. The importance of the PSED was emphasised in *R (Elias) v Secretary of State for Defence* [2006] EWCA Civ 1293, [2006] 1 WLR 3213, at [274], where Arden LJ (as she then was) said:

“It is the clear purpose of section 71 [the predecessor to section 149] to require public bodies ... to give advance consideration to issues of race discrimination before making any policy decision that may be affected by them. This is a salutary requirement, and this provision must be seen as an integral and important part of the mechanisms for ensuring the fulfilment of the aims of anti-discrimination legislation. ...”

181. We acknowledge that what is required by the PSED is dependent on the context and does not require the impossible. It requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex.
182. We also acknowledge that, as the Divisional Court found, there was no evidence before it that there is any reason to think that the particular AFR technology used in this case did have any bias on racial or gender grounds. That, however, it seems to us, was to put the cart before the horse. The whole purpose of the positive duty (as opposed to the negative duties in the Equality Act 2010) is to ensure that a public authority does not inadvertently overlook information which it should take into account.
183. Against that background of principle we turn to examine the reasons given by the Divisional Court for rejecting this ground of challenge. There are two aspects of the present case which particularly impressed the Divisional Court.
184. The first was the fact that there is a “human failsafe” component in the way in which AFR Locate is used. This means that a positive match made by the automated system will never by itself lead to human intervention. Before such an intervention (for example a stop of a member of the public for a conversation with a police officer) can



take place, there must be two human beings, including at least one police officer, who have decided to act on the positive match.

185. We do not consider the “human failsafe” is sufficient to discharge the PSED. As a matter of principle, it is not material to the PSED, which as we have observed, is a duty as to the process which needs to be followed, not what the substance of the decision should be. Secondly, as was acknowledged at the hearing before us, human beings can also make mistakes. This is particularly acknowledged in the context of identification. We would note the well-known warnings which need to be given to juries in criminal trials about how identification can be mistaken, in particular where a person has never seen the person being identified before: see *R v Turnbull* [1977] QB 224. Further, and in any event, this feature of the present case does not seem to us to go to the heart of the Appellant’s complaint under Ground 5, which is that SWP have not obtained information for themselves about the possible bias which the software they use may have.
186. The second matter which impressed the Divisional Court was the witness statement of PC Dominic Edgell, who found that there was virtually no difference in the statistics as to race or gender. We have considered that evidence.
187. Mr Edgell reviewed the AFR Locate deployments from after the UEFA Champions League Final of 2017 through to June 2018. During those deployments 290 alerts were generated. 82 were true positives and 208 were false positives. He says that it is important to note that these statistics are only of the persons who have generated an alert. The identity of those who passed the camera without generating an alert is unknown.
188. 188 of the alerts were males (65%). Of the 188 male alerts, 64 (34%) were true positives and 124 (66%) were false positives. In relation to females, of 102 alerts, 18 (18%) were true positives and 84 (82%) were false positives. A number of the female false alerts were matched against primarily two individuals who the AFR software provider would refer to as a “lamb”. A lamb is a person whose face has such generic features that may match much more frequently.
189. Mr Edgell also reviewed the ethnicity of those who were the subject of an alert. Of the true positives (82) 98% were “white north European”. Of the false positives (208) 98.5% were “white north European”.
190. Mr Edgell therefore concludes, at para. 26:

“From my experience and the information available to me, I have seen no bias based on either gender or ethnicity. ...”
191. In our view, this does not constitute a sufficient answer to the challenge based on the PSED. As Mr Squires submitted, Mr Edgell was dealing with a different set of statistics. He did not know, for obvious reasons, the racial or gender profiles of the total number of people who were captured by the AFR technology but whose data was then almost immediately deleted. In order to check the racial or gender bias in the technology, that information would have to be known. We accept Mr Beer’s submission that it is impossible to have that information, precisely because a safeguard

in the present arrangements is that that data is deleted in the vast majority of cases. That does not mean, however, that the software may not have an inbuilt bias, which needs to be tested. In any event, with respect to Mr Edgell, he is not an expert who can deal with the technical aspects of the software in this context.

192. We should address another submission which was made to us by Mr Beer for SWP although it did not feature in the reasoning of the Divisional Court. This submission arises from the scientific evidence which has been filed in these proceedings.
193. When the claim for judicial review was first lodged, reliance was placed in the Statement of Facts and Grounds on the first witness statement of Dr Anil Jain, dated 30 September 2018. Dr Jain is a professor in the Department of Computer Science and Engineering at Michigan State University in the United States. In his first witness statement he explains that the performance of AFR technology is affected by a number of variables, including “training datasets”: see para. 38(a). What this means is that the particular software which is used is “trained”. At para. 47, Dr Jain says that the accuracy of an AFR system depends to a considerable extent on the training dataset. He goes on to say, at para. 48, that AFR systems can suffer from training “bias”. At para. 49, he says that one cause of such training bias can be any imbalance in the demographic of subjects in the training datasets, resulting in the AFR system having a high false alarm rate or a high false reject rate for that particular demographic. At para. 51 Dr Jain states that it would appear that SWP were not aware of the dataset used to train the AFR system in this case. For that reason, he states, it would be difficult for SWP to confirm whether the technology is in fact biased. As a minimum for confirming whether an AFR system is biased, the database statistics, such as the number of males to females, and different races considered, would need to be known.
194. At the hearing before us Mr Beer placed particular reliance on a witness statement, filed in response to the first witness statement of Dr Jain, by Mr Paul Roberts, dated 23 November 2018. The first point to note about Mr Roberts’ statement is that it was obtained in response to the challenge brought in the present proceedings; it was not obtained proactively by SWP in order to fulfil the PSED.
195. Mr Roberts was employed by NEC (UK) Ltd as Head of Products and Solutions for Facial Recognition and is now employed by Northgate Public Services (UK) Ltd as Head of Global Facial Recognition. Both companies are subsidiaries of NEC Corporation. One of the products of the business is the NeoFace Watch software with which the present case is concerned.
196. Mr Roberts makes the point in his witness statement that Dr Jain’s report gave a generic description of generally available AFR software in the marketplace but is not a fully accurate description of NeoFace Watch. He states that the NeoFace algorithm is trained in laboratories and, on a typically annual basis, a new version of the algorithm is released containing improvements from, amongst other things, additional training. No further training is carried out by the system in any customer environments: see para. 10 of his witness statement. At para. 20, Mr Roberts states that the precise makeup, scale and sources of the training data used are commercially sensitive and cannot be released. He was, however, able to share certain facts, which he sets out in the following paragraphs. At para. 22 he states that:

“To minimise any impact of bias as a result of gender, the NeoFace Algorithm training data set contains roughly equal quantities of male and female faces.”

At para. 24 he states that the NeoFace Algorithm training data includes a wide spectrum of different ethnicities and has been collected from sources in regions of the world to ensure a comprehensive and representative mix. He states that great care, effort and cost is incurred by NEC, as a socially responsible major corporation, to ensure that this is the case.

197. Dr Jain responded to Mr Roberts’ statement in a second witness statement dated 25 January 2019. He fairly acknowledges, at para. 15, that he cannot comment on whether AFR Locate has a discriminatory impact as he does not have access to the datasets on which the system is trained and therefore cannot analyse the biases in those datasets. He goes on to say, however, that bias has been found to be a feature of common AFR systems and that SWP themselves are not in a position to evaluate the discriminatory impact of AFR Locate.
198. At paras. 24-28, Dr Jain specifically responds to the witness statement of Mr Roberts. He expresses the opinion that what Mr Roberts says is not sufficient to be able to determine that the NeoFace algorithm is not biased towards a particular demographic group. To make this determination, he says, a thorough evaluation needs to be done of the demographic composition of the NeoFace algorithm training dataset. Dr Jain states at para. 28, without that information SWP are not able to assess whether the training dataset is biased or may be.
199. We acknowledge that it is not the role of this Court to adjudicate on the different points of view expressed by Mr Roberts and Dr Jain. That would not be appropriate in a claim for judicial review, still less on appeal. The fact remains, however, that SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex. There is evidence, in particular from Dr Jain, that programs for AFR can sometimes have such a bias. Dr Jain cannot comment on this particular software but that is because, for reasons of commercial confidentiality, the manufacturer is not prepared to divulge the details so that it could be tested. That may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty under section 149.
200. Finally, we would note that the Divisional Court placed emphasis on the fact that SWP continue to review events against the section 149(1) criteria. It said that this is the approach required by the PSED in the context of a trial process. With respect, we do not regard that proposition to be correct in law. The PSED does not differ according to whether something is a trial process or not. If anything, it could be said that, before or during the course of a trial, it is all the more important for a public authority to acquire relevant information in order to conform to the PSED and, in particular, to avoid indirect discrimination on racial or gender grounds.
201. In all the circumstances, therefore, we have reached the conclusion that SWP have not done all that they reasonably could to fulfil the PSED. We would hope that, as AFR is a novel and controversial technology, all police forces that intend to use it in the future

would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias.

202. For the above reasons this appeal will be allowed on Ground 5.

### **Procedural matters**

203. For the sake of completeness we mention briefly two procedural matters which were before us at the hearing of the appeal. They both relate to applications to refer to new material, which was not before the Divisional Court because it did not exist at that time. This Court has a discretion to permit such evidence under CPR 52.21(2). It is well-established that the discretion is to be exercised having regard to the criteria in *Ladd v Marshall* [1954] 1 WLR 1489: see *Terluk v Berezovsky* [2011] EWCA Civ 1534, at [31]-[32] (Laws LJ).

204. The first request (no formal application being thought to be necessary) was made on behalf of the Information Commissioner to refer to two documents which have been issued by her since the judgment of the Divisional Court. The first of those documents is ‘The Use of Live Facial Recognition Technology by Law Enforcement in Public Places’ (31 October 2019). The other document is an ‘appropriate policy document’ template in relation to law enforcement processing under Part 3 of the DPA 2018.

205. Mr Beer did not object to our looking at these documents in general terms, although he did object insofar as reference might be made to any matter of fact which was not before the Divisional Court. While we found the first document interesting, it did not affect our decision or our reasons in this appeal. We have considered the ‘appropriate policy document’ template in relation to Ground 4 for the reasons we set out in paras. 160 and 161 of this judgment, which reflect the decision of the Divisional Court in paras. [139]-[141] of their judgment.

206. The other procedural matter to be addressed is an application on behalf of the Surveillance Camera Commissioner to adduce fresh evidence in the form of a letter dated 4 December 2019 which was sent to the Secretary of State by, amongst others, the Surveillance Camera Commissioner. This was said to be relevant to an issue mentioned by the Divisional Court in its judgment, at [44], where reference was made to the fact that the Secretary of State has set up an Oversight and Advisory Board (“the Board”), comprising representatives from the police and other bodies, including the Surveillance Camera Commissioner, “to coordinate consideration of the use of facial imaging and AFR by law enforcement authorities.” As we understand it, a disagreement has arisen since the judgment of the Divisional Court between the Surveillance Camera Commissioner and the Secretary of State as to the role performed by the Board.

207. On behalf of the Secretary of State objection was taken to the admissibility of this evidence by Mr O’Brien, although he was content that we should look at it on a contingent basis.

208. We need not take time over this procedural dispute. It seems to us that Mr O’Brien was right to submit that the setting up of the Board was at most a peripheral point, mentioned in passing in the Divisional Court’s judgment. It does not seem to us to have had any

material impact on that Court's judgment: in particular, that Court made no reference to the existence of the Board in its reasoning on the issue of whether the interference with Article 8 rights was in accordance with the law. In any event, it does not affect this Court's conclusions or reasoning in this appeal. For that reason we refuse the application to adduce fresh evidence on behalf of the Surveillance Camera Commissioner.

## **Conclusion**

209. For the reasons we have given this appeal will be allowed on Grounds 1, 3 and 5. We reject Grounds 2 and 4.
210. As to the appropriate remedy, we consider that declaratory relief to reflect the reasons why this appeal has succeeded will suffice. In the circumstances which have arisen, the parties agree that the only remedy which is required is a declaration but they have not been able to agree the precise terms of a declaration. Having considered the rival contentions, we have concluded that the declaration proposed by SWP more accurately reflects the judgment of this Court. We will grant a declaration in the following terms:
- 1) The Respondent's use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis, which engaged Article 8(1) of the European Convention on Human Rights, was not in accordance with the law for the purposes of Article 8(2).
  - 2) As a consequence of the declaration set out in paragraph 1 above, in respect of the Respondent's ongoing use of Live Automated Facial Recognition technology, its Data Protection Impact Assessment did not comply with section 64(3)(b) and (c) of the Data Protection Act 2018.
  - 3) The Respondent did not comply with the Public Sector Equality Duty in section 149 of the Equality Act 2010 prior to or in the course of its use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis.

## **ANNEX A**

### **LEGAL FRAMEWORK**

#### **Legislation**

##### *Data Protection Act 1998 ("DPA 1998")*

1. Section 1(1) of the DPA 1998 defined "personal data" as:

“... data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller”.
2. Section 1(1) of the DPA 1998 defined "data processing" as:

“... obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data” [with a range of non-exhaustive examples given].
3. Section 4(4) provided that it was:

“... the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller” [subject to section 27(1) concerning the exemptions].
4. The data protection principles were set out in Schedule 1 to the DPA 1998:
  - (1) Principle 1 is that personal data shall be processed fairly and lawfully and, in particular, shall not be “processed” at all unless it is necessary for a relevant purpose (referred to in Schedule 2 below). In the case of the police, the relevant purposes are the administration of justice and the exercise of any other function of a public nature exercised in the public interest.
  - (2) Principle 2 is that personal data may be obtained only for lawful purposes and may not be further “processed” in a manner incompatible with those purposes.
  - (3) Principle 3 is that the data must be “adequate, relevant and not excessive” for the relevant purpose.
  - (4) Principle 4 is that data shall be accurate and, where necessary, kept up to date.
  - (5) Principle 5 is that the data may not be kept for longer than is necessary for those purposes.
  - (6) Principle 6 is that personal data shall be processed in accordance with the rights of data subjects under this Act.
  - (7) Principle 7 is that proper and proportionate technical and organisational measures must be taken against the unauthorised or unlawful “processing” of the data.

(8) Principle 8 is that personal data shall not be transferred outside the European Economic Area unless the country ensures an adequate level of protection.

5. Schedule 2 included the following conditions:

“1. The data subject has given his consent to the processing.

...

5. The processing is necessary—

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.”

6. The DPA 1998 did not contain any definition of biometric data; nor was such data included within the definition of sensitive personal data within section 2 of the DPA 1998.

Protection of Freedoms Act 2012 ("PFA 2012")

7. Chapter I of Part 2 of the PFA 2012 makes provision for the “Regulation of CCTV and Other Surveillance Camera Technology”. The relevant provisions of the PFA 2012 relate to the overt use of “surveillance camera systems” in public places by “relevant authorities” in England and Wales.

8. Section 29(1) mandates the Secretary of State to prepare a code of practice containing guidance about surveillance camera systems. Section 29(5) requires consultation with the National Police Chief's Council, the Information Commissioner, the Investigatory Powers Commissioner, the Surveillance Camera Commissioner, the Welsh Ministers and other persons the Secretary of State considers appropriate.

9. Section 29(6) provides that a surveillance camera system means:

“(a) closed circuit television or automatic number plate recognition systems,

(b) any other systems for recording or viewing visual images for surveillance purposes,

(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or

(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).” (emphasis added)

10. A surveillance camera system which makes use of AFR therefore falls within this definition and is addressed within the Surveillance Camera Code of Practice.
11. Section 30 provides that the Secretary of State must lay the code of practice and order providing for the code to come into force before Parliament, and that such an order is to be a statutory instrument.
12. Section 31 provides that the Secretary of State must keep the code under review and may alter or replace it.
13. Section 33 requires “relevant authorities” (which includes a chief officer of a police force) to have regard to the code of practice when exercising any functions to which it relates.
14. Section 33 further sets out the responsibility of a relevant authority as follows:
  - “(1) A relevant authority must have regard to the surveillance camera code when exercising any functions to which the code relates.
  - (2) A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings.
  - (3) The surveillance camera code is admissible in evidence in any such proceedings.
  - (4) A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings.” (emphasis added)
15. Section 33(5) provides the list of “relevant authorities” for the purposes of this part of the Act. Section 33(5)(j) sets out the inclusion of any chief officer of a police force in England and Wales. The Chief Constable of South Wales Police is therefore a relevant authority for the purposes of this Act.
16. Section 34 provides for the appointment of a Surveillance Camera Commissioner by the Secretary of State. The Surveillance Camera Commissioner is an arms-length body funded by, but independent of, the Home Office. His role is, *inter alia*, to ensure public confidence in surveillance systems. Section 34 provides that the Commissioner's functions include:
  - “(a) Encouraging compliance with the surveillance camera code;
  - (b) Reviewing the operation of the code; and



(c) Providing advice about the code (including changes to it or breaches of it).”

17. 17. The Secretary of State issued and published a code of practice pursuant to ss.30 and 32 of the PFA 2012 in June 2013 as the Surveillance Camera Code of Practice (see further below).

Data Protection Act 2018 (“DPA 2018”)

18. 18. The DPA 2018 came into force on 25th May 2018.

19. 19. Section 29 of the DPA 2018 provides:

PART 3 LAW ENFORCEMENT PROCESSING

“29 Processing to which this Part applies

(1) This Part applies to—

(a) the processing by a competent authority of personal data wholly or partly by automated means, and

(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies. ...”

20. Section 34 of the DPA 2018 provides an overview of the six data protection principles and the duties of the data protection controller:

“34 Overview and general duty of controller

(1) This Chapter sets out the six data protection principles as follows—

(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);

(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);

(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);

(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);

(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);

(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).

(2) In addition—

(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and

(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.

(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.”

21. Section 35 of the DPA regulates "sensitive processing" and specifies the conditions that must be satisfied before it may take place. Section 35 provides as follows:

“35 The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

- (5) The second case is where—
- (a) the processing is strictly necessary for the law enforcement purpose,
  - (b) the processing meets at least one of the conditions in Schedule 8, and
  - (c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).
- (6) The Secretary of State may by regulations amend Schedule 8—
- (a) by adding conditions;
  - (b) by omitting conditions added by regulations under paragraph (a).
- (7) Regulations under subsection (6) are subject to the affirmative resolution procedure.
- (8) In this section, "sensitive processing" means—
- (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
  - (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
  - (c) the processing of data concerning health;
  - (d) the processing of data concerning an individual's sex life or sexual orientation."

22. Section 35 reflects the language and scope of Article 10 of the Data Protection Law Enforcement Directive (2016/680/EU).

*"Article 10 Processing of special categories of personal data*

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only..."

### *Definitions*

23. Section 3(2) of the DPA 2018 defines “personal data” as:

“...any information relating to an identified or identifiable living individual”, which means an individual “who can be identified, directly or indirectly, in particular by reference to—(a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual”.

24. Section 35(8) of the DPA 2018 defines “sensitive processing” as activities including:

“...the processing of... biometric data... for the purpose of uniquely identifying an individual.”

25. Section 205(1) of the DPA 2018 defines “biometric data” as:

“...personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data”.

### *Conditions*

26. Section 35(5) prescribes conditions which must be satisfied before the processing of biometric data for law enforcement purposes may be permitted. These conditions are threefold: (a) the processing is strictly necessary for the law enforcement purpose; (b) the processing meets at least one of the conditions in Schedule 8; and (c) the controller has an appropriate policy document in place (see section 42).

27. The Schedule 8 conditions include:

“1. Statutory etc purposes

This condition is met if the processing-

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

2. Administration of justice

This condition is met if the processing is necessary for the administration of justice.

...

6. Legal claims

This condition is met if the processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)..."

28. Section 42 contains requirements in respect of the "appropriate policy document" referred to in section 35(4), that must be in place:

**"42 Safeguards: sensitive processing**

(1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on... a condition specified in Schedule 8).

(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which—

(a) explains the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and

(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period—

(a) retain the appropriate policy document,

(b) review and (if appropriate) update it from time to time, and

(c) make it available to the Commissioner, on request, without charge.

(4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—

(a) ...which condition in Schedule 8 is relied on,

(b) how the processing satisfies section 35 (lawfulness of processing), and

(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.

(5) In this section, “relevant period”, in relation to sensitive processing ...in reliance on a condition specified in Schedule 8, means a period which—

(a) begins when the controller starts to carry out the sensitive processing ...in reliance on that condition, and

(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out the processing.”

29. Section 64 of the DPA 2018 provides:

**“Data protection impact assessment**

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.”

## **Code and Guidance**

### *Secretary of State's Surveillance Camera Code of Practice*

30. The Surveillance Camera Code of Practice (“SC Code”) was issued by the Secretary of State in June 2013. There is a statutory obligation to have regard to that code when exercising any functions to which the code relates (see s.33 of the PFA 2012 above). The SC Code lays down a series of 12 “Guiding Principles” for the operators of surveillance camera systems. They are as follows:

“1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.”

31. The SC Code concerns “conventional” CCTV systems, but specifically addresses the use of AFR as part of a surveillance camera system (see paragraph 3.2.3 below). The SC Code also covers the broader spectrum of statutory and procedural considerations which apply to surveillance camera operators, including Human Rights, Data Protection, Investigatory Powers and the forensic integrity of images.

32. Relevant paragraphs from the SC Code are as follows (with emphasis added):

“1.8 This code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places.”

“2.1 Modern and forever advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images and information. This technology can be a valuable tool in the management of public safety and security, in the protection of people and property, in the prevention and investigation of crime, and in bringing crimes to justice. Technological advances can also provide greater opportunity to safeguard privacy. Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need.”

“2.2 In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with the right provided that the interference is in pursuit of a legitimate aim and the interference is proportionate. Amongst the qualified rights is a person's right to respect for their private and family



life, home and correspondence, as provided for by Article 8 of the ECHR.”

“2.3 That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential, now and in the future. In considering the potential to interfere with the right to privacy, it is important to take account of the fact that expectations of privacy are both varying and subjective. In general terms, one of the variables is situational, and in a public place there is a zone of interaction with others which may fall within the scope of private life. An individual can expect to be the subject of surveillance in a public place as CCTV, for example, is a familiar feature in places that the public frequent. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place.”

“2.4 The decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented as the stated purpose for any deployment. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. Decisions over the most appropriate technology should always take into account its potential to meet the stated purpose without unnecessary interference with the right to privacy and family life. Furthermore, any deployment should not continue for longer than necessary.”

“3.2.3 Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated<sup>4</sup>. It should always involve human intervention before decisions are taken that affect an individual adversely.” (Footnote 4: “The Surveillance Camera Commissioner will be a source of advice on validation of such systems.”)

“4.8.1 Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body-worn video recorders.”

“4.12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by

others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.”

“4.12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on a reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.”

### Surveillance Camera Commissioner's AFR Guidance

33. The Surveillance Camera Commissioner has published “guidance” or “advice” on the use of AFR by the police in conjunction with CCTV entitled “The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems” (“the AFR Guidance”). The guidance explains the roles of the Surveillance Camera Commissioner and Information Commissioner in relation to the regulation of the police use of AFR. The Surveillance Camera Commissioner AFR Guidance is designed to assist relevant authorities in complying with their statutory obligations “arising under section 31(1)” of the PFA 2012 and the SC Code (paragraph 1.3).
34. The AFR Guidance was promulgated on the basis that the Surveillance Camera Commissioner “should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems” (SC Code, paragraph 5.6). It is said that the AFR Guidance indicates “the way in which the Commissioner is minded to construe the particular statutory provisions arising from PFA 2012 and those provisions within the Code of Practice in the absence of case law” (paragraph 1.8).
35. The AFR Guidance focuses on the assessment of the necessity and proportionality of deployments of AFR. It also provides advice on conducting risk assessments and making use of the Surveillance Camera Commissioner's ‘Self-Assessment Tool’. In respect of watchlists there are suggestions concerning the nature of images used to produce watchlists.
36. Unlike the SC Code, there is no requirement for SWP to have regard to the AFR Guidance. This guidance was first published in October 2018 and re-published without changes in March 2019 (i.e. after the two deployments of AFR about which the Appellant complains).

### SWP Documents

#### SWP Policy Document

37. SWP have issued a policy document entitled “Policy on Sensitive Processing of Law Enforcement Purposes, under Part 3 Data Protection Act 2018” (Version 2.0, November 2018) (“the November 2018 Policy Document”). That Policy Document sets out SWP's policy as regards compliance with the six Data Protection Principles in Part 3 of the DPA 2018:

#### **“3. Compliance with Data Protection Principles**

**a) 'lawfulness and fairness'**

The lawfulness of South Wales Police processing is derived from its official functions as a UK police service, which includes the investigation and detection of crime and the apprehension of offenders, including acting in obedience to court warrants that require the arrest of defendants who have failed to attend court.

**b) 'data minimisation'**

South Wales police only processes sensitive personal data when permitted to do so by law. Such personal data is collected for explicit and legitimate purposes such as biometric data during the deployment of Automatic Facial Recognition technology.

**c) 'accuracy'**

During AFR Locate deployments South Wales Police collects the information necessary to determine whether the individual is on a watchlist. If an intervention is made the process will not prompt data subjects to answer questions and provide information that is not required.

Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified data sets.

**d) 'storage limitation'**

Providing complete and accurate information is required when constructing a watchlist. During AFR Locate deployments watchlists will be constructed on the day of deployment and where the deployments extend beyond 24 hours these will be amended daily. Where permitted by law and when it is reasonable and proportionate to do so, South Wales Police may check this information with other organisations – for example other police and law enforcement services. If a change is reported by a data subject to one service or a part of South Wales Police, whenever possible this is also used to update the AFR application, both to improve accuracy and avoid the data subject having to report the same information multiple times.

**e) 'integrity and confidentiality'**

South Wales Police has a comprehensive set of retention policies in place which are published online, further information specific to AFR can be found on SWP AFR webpage.

All staff handling South Wales Police information are security cleared and required to complete annual training on the importance of security, and how to handle information appropriately.

In addition to having security guidance and policies embedded throughout SWP business, SWP also has specialist security, cyber and resilience staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.”

SWP Standard Operating Procedures (“SOP”)

38. SWP has Automatic Facial Recognition SOP which apply to their use of AFR. They were published in November 2018 (i.e. after the dates of the 2 events in question), when a separate facial recognition section was added to SWP's website, and the SOPs were published on that webpage. The SOP's primary features include (see especially pages 6 and 14):

(1) A stipulation that watchlists should be “proportionate and necessary” for each deployment and primary factors for the inclusion on watchlists include will be “watchlist size, image quality, image provenance and rationale for inclusion”.

(2) The numbers of images included within a watchlist cannot exceed 2,000 due to contract restrictions “but in any event1 in 1000 false positive alert rate should not be exceeded”.

(3) Children under the age of 18 will not normally feature in a watchlist due to “the reduced accuracy of the system when considering immature faces”.

(4) The decision for an AFR deployment wherever possible will ultimately be made by the Silver Commander.

(5) The rationale for the deployment of AFR is to be recorded in a pre-deployment report.

(6) Signs advertising the use of the technology are to be deployed to ensure that where possible an individual is aware of the deployment before their image is captured.

(7) Interventions are not to be made on the basis of a similarity score alone and when an intervention is made intervention officer will establish the identity of the individual by traditional policing methods.

(8) Details of the retention of different types of information gathered during an AFR deployment.

SWP Operational Advice

39. SWP have also issued guidance in the form of “Operational Advice for Police Trials of Live Facial Recognition” for use by officers conducting the trials which has been submitted to the National Police Chiefs Council.



## South Wales Police Live Facial Recognition (LFR): Legal Mandate

Summary: Outlines the legal basis for the SWP use of LFR technology

|               |                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------|
| Name of Force | South Wales Police (SWP)                                                                        |
| Subject       | Live Facial Recognition (LFR)                                                                   |
| Summary       | Outlines the legal basis for SWP's use of overt LFR technology to locate persons on a Watchlist |
| Author        | Ch Insp Scott Lloyd                                                                             |

|                              |                               |
|------------------------------|-------------------------------|
| Project Name                 | Facial Recognition Technology |
| Senior Responsible Office-   | ACC Mark Travis               |
| Business Area/Department     | Digital Services Division     |
| Proposed implementation date | Immediately                   |

### Change control:

| Version | Date     | Authority         | Evidence of approval   | Record of change |
|---------|----------|-------------------|------------------------|------------------|
| 0.1     | 30.03.21 | Project Lead      | Ch. Insp Scott Lloyd   | Initial Draft    |
| 0.2     | 08.06.21 | DSD SMT           | Ch. Supt Simon Belcher | No Amendments    |
| 0.3     | 01.11.21 | Project Lead      | Ch. Insp Scott Lloyd   | Minor Amendments |
| 1.0     | 11.11.21 | SRO               | ACC Mark Travis        | No Amendments    |
| 1.1     | 03.03.22 | Project Lead      | Ch. Insp Scott Lloyd   | ICO amendments   |
| 1.2     | 01.05.23 | Project Oversight | Ch. Insp Scott Lloyd   | Amendments       |

|           |                                                       |           |
|-----------|-------------------------------------------------------|-----------|
| <b>1</b>  | <b><i>Introduction</i></b>                            | <b>3</b>  |
| <b>2</b>  | <b><i>Common Law</i></b>                              | <b>4</b>  |
| <b>3</b>  | <b><i>Police and Criminal Evidence Act 1984</i></b>   | <b>5</b>  |
| <b>4</b>  | <b><i>Human Rights Act 1998</i></b>                   | <b>5</b>  |
| <b>5</b>  | <b><i>Equality Act 2010</i></b>                       | <b>15</b> |
| <b>6</b>  | <b><i>Data Protection Act 2018</i></b>                | <b>17</b> |
| <b>7</b>  | <b><i>General Data Protection Regulation</i></b>      | <b>21</b> |
| <b>8</b>  | <b><i>Protection of Freedoms Act 2012</i></b>         | <b>22</b> |
| <b>9</b>  | <b><i>Freedom of Information Act 2000</i></b>         | <b>23</b> |
| <b>10</b> | <b><i>Legal Framework and Governance Overview</i></b> | <b>23</b> |

**Terms & Definitions: Capitalised terms used in this South Wales Police LFR Legal Mandate shall have the meaning given to them in the South Wales Police LFR Policy Document unless otherwise defined in this South Wales Police LFR Legal Mandate.**

## 1 Introduction

- 1.1 LFR for law enforcement purposes is not subject to dedicated primary legislation. LFR is regulated by a number of sources of primary and secondary legislation as well as both national and local policy. This ‘tapestry’ of legislation combine to provide a multi-layered legal structure to use and regulate the use of LFR.

|                                  |                                             |                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tier one:<br>Legislation         | Legal Power to use LFR                      | <ul style="list-style-type: none"> <li>a) Common Law</li> <li>b) Police and Criminal Evidence Act 1984 Code D (revised)</li> </ul>                                                                                                                                                                                                                                               |
|                                  | Regulating the use of LFR                   | <p><b>Operational</b></p> <ul style="list-style-type: none"> <li>b) Human Rights Act 1998</li> <li>c) Equality Act 2010</li> </ul> <p><b>Data Management</b></p> <ul style="list-style-type: none"> <li>d) Data Protection Act 2018 (Part 3)</li> <li>e) UK General Data Protection Regulation</li> <li>f) Protection of Freedoms Act 2012</li> </ul>                            |
|                                  | Requests for Information in relation to LFR | <ul style="list-style-type: none"> <li>g) Freedom of Information Act 2000</li> <li>h) Data Protection Act 2018 (Subject Access Requests)</li> </ul>                                                                                                                                                                                                                              |
| Tier Two:<br>Code and Guidance   | Regulating the use of LFR                   | <ul style="list-style-type: none"> <li>a) Secretary of State’s Surveillance Camera Code of Practise.</li> <li>b) Guidance issued by the Surveillance Camera Commissioner (Facing the Camara)</li> <li>c) Information Commissioner’s Office Code of Practise for Surveillance Cameras and associated guidance issued by the Information Commissioner</li> </ul>                   |
| Tier Three:<br>SWP LFR Documents | Regulating the use of LFR                   | <ul style="list-style-type: none"> <li>a) SWP Policy Document</li> <li>b) SWP Standard Operating Procedures</li> <li>c) SWP Training Documents</li> <li>d) SWP Data Protection Appropriate Policy Document</li> <li>e) Data Protection Impact Assessment</li> <li>f) Equality Impact Assessment</li> <li>g) Community Impact Assessment</li> <li>h) SWP Legal Mandate</li> </ul> |

## 2 Common Law

2.1 The police have a number of long-established policing responsibilities and powers derived from common law which have been recognised by the courts. SWP is obliged to comply with common law and statutory safeguards in delivering its policing operational duties and relies on common law to discharge a number of its duties.

2.2 Key common law powers SWP may rely on when utilising LFR technology include the policing common law powers to:

- (a) protect life and property;
- (b) preserve order and prevent threats to public security;
- (c) prevent and detect crime;
- (d) bring offenders to justice; and
- (e) uphold national security.

Example: SWP has detailed uses of LFR as a policing tactic for locating those who are wanted for an outstanding warrant. In this context the use of LFR technology to facilitate officers to promptly locate those evading arrest would enable SWP to discharge its responsibilities to protect life and property. It would also be compatible with SWP's duty to bring offenders to justice by facilitating a prompt and effective investigation.

2.3 The use of SWP's common law power as a legal basis to support the deployment use of LFR has been considered and recognised in the 'Bridges' case:

- a) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) (the "High Court Bridges" decision); and then on Appeal in,
- b) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision).

The Court of Appeal further summarised the legal basis in relation to compilation of Watchlists as being "both authorised under the Police and Criminal Evidence Act 1984 and within the powers of police at common law." The reference to the 1984 Act is a reference to imagery obtained pursuant to Section 64A (*Photographing of suspects etc.*) of the Act and particularly section 64A(4)(a) which allows a photograph taken under the section to be "used ... for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence". The Court of Appeal notes that "this was not an issue which we have to address in this appeal, since it is now common ground that SWP do have the power to deploy [LFR]."

**Authorising Officers:** When considering the use of LFR technology, must be clear as to the common law policing power that is relied upon for lawfully authorising the use of LFR and record this as part of the decision-making process.



### 3 Police and Criminal Evidence Act 1984

- 3.1 Section 64A of PACE allows photographing a person who is detained at a station.
- 3.2 Allows for the photographs to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions.

### 4 Human Rights Act 1998

- 4.1 SWP use of LFR must be in compliance with the Human Rights Act 1998. LFR technology engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

'There shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.'

- 4.2 As a qualified right, any interference with an individual's Article 8 rights is only permissible if:

- a) there is a **legal basis** for the interference with the qualified right that the public can understand;
- b) the use of LFR seeks to achieve the **legitimate aim**;
- c) it is **necessary** for the purposes of that aim in a democratic society; and
- d) the use of LFR is **proportionate** to the legitimate aim being sought.

- 4.3 It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom*<sup>1</sup> confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that LFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".<sup>2</sup>

- 4.4 The High Court and Court of Appeal Bridges cases considered Article 8, specifically in the context of LFR technology and confirmed that Article 8 is engaged in so far as someone passes through the Zone of Recognition and in so far as someone is placed on a LFR Watchlist for a Deployment. Depending on the nature of the deployment, the then Surveillance Camera Commissioner has identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms. Authorising Officers should contact SWP Special Legal Casework should they consider a proposed deployment may have a wider human rights point to consider.

---

<sup>1</sup> (2009) 48 EHRR 50, at [66 and 67]

<sup>2</sup> At [104]

#### 4.5 There is a legal basis for the interference with the qualified right that the public can understand

LFR will be used to allow the SWP to discharge its well established operational duties pursuant to common law. The courts have recognised that “the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them”.<sup>3</sup>

In the case of *R (Catt) v Chief Police Officers [2015] A.C. 1065*, Lord Sumption recognised that applicants could have their personal information noted down and retained by the police as they occupied publically accessible space. The court recognised the police’s common law powers to collect and store information are subject to an “intensive regime of statutory and administrative regulation” under the Data Protection Act and various guidance documents on the management of police information.

The courts have further recognised the right of the police to make use of a photograph of an individual. The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect’s accomplice or of anyone else. The court confirmed the “key is that they must have these and only these purposes in mind and must ... make no more than reasonable use of the picture in seeking to accomplish them”.<sup>4</sup>

4.6 In the case of the SWP’s use of LFR, the LFR Legal Framework outlines the legal basis for any interference with an individual’s Article 8 rights. The High Court Bridges case confirmed the police’s common law policing powers to be “amply sufficient” in relation to this type of use of LFR and confirmed that “the police do not need new express statutory powers for this purpose”. This was further considered in the Court of Appeal Bridges case which also recognised the sufficiency of the legal framework, noting<sup>5</sup>:

*“the legal framework which regulates the deployment of [SWP’s use of LFR] does contain safeguards which enable the proportionality of the interference with Article 8 rights to be adequately examined.”*

4.7 The Court of Appeal Bridges decision further noted that, to be ‘in accordance with the law’ the legal basis must:

*“be ‘accessible’ to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be ‘foreseeable’ meaning that it must be possible for a person to foresee its consequences for them and it should not ‘confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself’.”*

4.8 In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held in the case before it to determine *where* they

---

<sup>3</sup> *R (Catt) v Association of Chief Police Officers [2015] A.C. 1065* at [11].

<sup>4</sup> Per Laws J in *Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804* at 810F

<sup>5</sup> At [69].

deployed facial recognition technology and *who* they deployed it to locate those on a Watchlist. The court refers to this as the “Who Question” and the “Where Question”.

- a) The ‘Who’ Question: When considering how the ‘Who Question’ should be answered, the Court of Appeal made it clear that, the law does not seek specific confirmation as to who is on a Watchlist (they recognise the NCND principle<sup>6</sup>). The Court of Appeal recognised that individuals could be added to a Watchlist on the basis that they are wanted on suspicion of an offence, wanted on warrant and vulnerable persons”.
- b) The Court of Appeal also explains why a category of those “other persons where intelligence is required” was not accessible and foreseeable to meet the ‘in accordance with the law’ test. They noted that the category was not readily understood, nor was it objective – it left “too broad a discretion vested in the individual police officer to decide who should go onto the watchlist” – essentially it allowed police officers to decide what ‘other persons where intelligence is required’ meant on a case-by-case basis rather than deciding if a subject met the criteria set out in the force policy.
- c) Following an approach recognised by the Court of Appeal<sup>7</sup>, SWP addresses the ‘Who Question’ in its published SWP LFR Documents, particularly at Section 6 of the SWP SOP. SWP sets the criteria that applies to govern the images that may be included on a Watchlist and in what circumstances. To ensure the Watchlisting criteria is accessible and foreseeable, SWP explains terminology such as ‘presenting a risk of harm’ and ‘otherwise of interest to the police’ such that they can be readily understood and objective to both officers and the public. It sets out the standard required for inclusion on a Watchlist, linking the necessity and criteria for the inclusion on a Watchlist with the policing need and the proportionality of taking any action.
- d) The ‘Where Question: The Court of Appeal noted that the South Wales Police team “was not able to draw to our attention anything which specifies where AFR Locate may be deployed”. SWP LFR Documents answers this question, particularly the SWP LFR SOP at Section 5. In answering this question, in many instances, the need to locate a person will determine where it is best to site LFR to facilitate making a successful location. However, other factors will also be relevant and these include the nature of the site itself from a privacy perspective, those passing the site, and the policing need to be at the site (including for the public’s protection, suppressing crime hotspots, and getting ahead of crime trends).

With the benefit of the *Bridge’s* decisions, the law has now been applied to the live use of facial recognition technology. These judicial decisions, taken together with the SWP’s published documentation to support the use of LFR allows the LFR Legal Framework principles to be predictably applied to the use of LFR in an accessible and understandable way. It allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards SWP operate to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

---

<sup>6</sup> At [95].

<sup>7</sup> At [118].

#### 4.9 The use of LFR seeks to achieve a legitimate aim

Article 8, recognises action in the interests of national security, public safety and the prevention of disorder and crime as legitimate aims. The use of LFR in the context of assisting SWP locate offenders will help SWP achieve its law enforcement purposes.

The means by which SWP may use LFR will be an operational decision within the parameters of the law and SWP LFR Documents. It will need to be driven by the policing issue at hand. This may vary from the need to locate those wanted in connection with criminality or otherwise pose a risk of harm, to more preventative tactics designed to bring reassurance to communities and enable the use of precision technology to more proactively focus policing resources.

**Authorising Officers:** At the point that it is decided to deploy LFR, the decision maker must be clear as to its purpose and how using LFR will help SWP realise a legitimate aim. In deciding if the use of LFR is a suitable way to achieve a legitimate aim, the decision maker must consider if benefits of using LFR justify its use for the legitimate aim when compared to any impact on the individual's Article 8 Rights.

#### 4.10 The use of LFR is *necessary* for the purposes of that legitimate aim in a democratic society

LFR will be used in response to a pressing social need by helping SWP combat crime in areas where LFR has the greatest potential to assist. It is a tool that helps SWP to discharge its operational responsibilities, primarily to help prevent and detect crime and protect the most vulnerable.

**Authorising Officers:** When considering the Deployment of LFR, its use is to be underpinned by an intelligence case to highlight the need to combat the relevant crime or public safety issue or policing need to deploy. Having identified a need, this will allow the Authorising Officer to consider the use of LFR. Authorising Officers must decide the use of LFR is *necessary* and not just desirable to enable SWP to achieve its legitimate aim. In deciding the use of LFR to be necessary, the issue which LFR was intending to address and how LFR would be deployed to address that problem.

The following are examples of why LFR may be used as a necessary tool to assist SWP in preventing crime and disorder. The examples are illustrative only and there will be other scenarios where the use of LFR is justified.

**Child sexual abuse:** The use of LFR will assist SWP in tackling child sexual abuse. LFR could be deployed based on intelligence to find vulnerable individuals who are missing and believed to be at risk of child sexual abuse. Equally LFR could be used at large crowded events known to be frequented by sexual predators in an attempt to identify and prevent similar attacks. Missing persons investigations use significant police resources where the need to locate is time critical. In such circumstances, it is of great importance to use all reasonable measures, to have the best chance of making a successful identification when the often

scarce identification opportunities arise. At times, the police may also enlist the public to help with locating missing people through the use of public appeals, by circulating a photograph of a vulnerable child across the media. This is a potentially much greater intrusion to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use LFR as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers SWP a route to discharge its common law responsibilities to protect life.

However, it should be noted that data protection law is not a barrier to information sharing.

**Personal property theft:** The use of LFR will assist SWP in fighting criminals targeting potentially young and vulnerable persons at music events. By way of example LFR could be deployed at music venues, LFR can act as a tool to assist police officers identify those persons connected to large scale personal property theft. LFR has the ability to have a Watchlist that can be scoped to focus on traveling criminals who follow bands across Europe with the sole purpose of engaging in criminal activity. Using LFR in this way would help SWP achieve its aim of preventing and detecting crime and disorder and protecting the public through the disruption of those seeking to commit thefts by making it more difficult to enter the location.

Additionally, in a climate where police forces need to operate efficiently, SWP has also identified that technology such as LFR can assist with the challenges of quickly and cost efficiently locating those with outstanding warrants or who have otherwise breached their bail conditions. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances. The High Court Bridges case supports that there is a "considerable additional benefit to the public interest to including those wanted on a warrant" for a Deployment of LFR, even when there is no specific intelligence to place them in the area of the Deployment. The intrusion to those passing the system is no greater, but (i) the potential to protect the public from those wanted by the courts, (ii) the results from Deployments where those with outstanding warrants were included and (iii) the resultant arrests justified the inclusion of those with outstanding warrants from the courts as a *necessary* action to bring offenders to justice.

#### 4.11 The use of LFR is proportionate to legitimate aim being sought

When considering the Deployment of LFR, the benefits of using LFR for an investigation or operation should not be disproportionate or arbitrary. In this respect the Surveillance Camera Commissioner recognises that:

*"used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".*

In this respect, the following factors (amongst others, depending on the nature of the Deployment) will guide Authorising Officers:

- a) *The use of LFR should be a reasonable use of SWP powers - it will not be proportionate if the proposed use of LFR is excessive in the overall circumstances of the investigation, operation or wider operational strategy to tackle a policing issue.*

Authorising Officers will need to consider the seriousness of the policing issues at hand and the potential benefits of using LFR and balance this with any wider impact its Deployment may have to those on a Watchlist and the public at large. This will allow a decision to be made as to whether LFR is appropriate for use. Authorising Officers must give consideration to the composition of the Watchlist compiled for the LFR system to match against, to ensure that it is not compiled in an excessive manner. The Watchlist needs to satisfy the necessity and proportionality test and will therefore be driven by the intelligence case and bespoke for each Deployment of LFR to ensure it meets the aims of each Deployment.

With this in mind, the Watchlist compiled for each Deployment of LFR should be current; based on those currently of interest to SWP and/or wider UK law enforcement to mitigate the risk of the LFR system matching with those no longer of interest to SWP and/or wider UK law enforcement.

- b) *Consideration should be given as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference.*

The use of LFR should be considered against other methods of locating persons of interest to SWP and/or UK Law Enforcement and other policing tactics which may help tackle the policing issue at hand. Consideration should be given as to the effectiveness and intrusiveness of other viable methods that could give the same result, with the least intrusive, viable method being adopted to progress an investigation or Deployment.

**Example:** Circulating a wanted image on social media may be considered as an alternative to the use of LFR.

The use of LFR can be targeted to a specific area and does not result in the public being made aware of the identity of a person being sought by the SWP. It can also be used for a limited period, targeted, based on wider intelligence, to times and places when it might be most expected to locate an individual.

By comparison, social media results in a person's image being put into the public domain in a less targeted way. Once online, the image is public and SWP no longer has control of that image. It therefore has potential to remain online even when the person has been traced and thus is a greater intrusion into the privacy of the individual being sought.

The Authorising Officer considering the use of LFR should balance any intrusion into privacy against the need for the investigative activity. If the Authorising Officer uses LFR in a way which minimises any impact it may have on a person's privacy as far as possible, it may offer a more appropriate, less intrusive alternative to a social media

**Authorising Officers:** When taking a decision to deploy LFR, Authorising Officers should record what other methods, as appropriate, were either not implemented or have been employed but which were assessed to be insufficient or inappropriate to fulfil SWP's aim.

- c) How and why the methods adopted will cause the least possible interference to the person(s) sought and others must be addressed.*

All uses of LFR under this Legal Mandate will be overt. LFR will be used for a limited time – with a limited footprint, with a defined purpose (controlled by way of SWP LFR Documents). The LFR system will be visibly deployed in an open and transparent way. Consistent with the principle of engaging with the public, SWP LFR Documents also provides a structure for awareness measures which respond to the nature and objectives of the use of LFR.

**Proportionality controls.** Controls are also designed in to the LFR system and its operation to help minimise any impact on the public and those placed on a Watchlist as follows:

- I. LFR cannot be used to locate persons unless they have been included on a Watchlist.
- II. The creation of any Watchlist is specific to the Deployment of LFR and informed by the intelligence case for the Deployment; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching.
- III. Images on a Watchlist will be lawfully held by SWP with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Watchlist.
- IV. Authorising Officers need to expressly consider and approve the use of non-police originated images on any Watchlist. This is because particular privacy considerations may attach to an image where it originates from outside of a policing context. For example, it may be that the image was not placed in the public domain, was taken in a place that attracts a higher expectation of privacy or is an image that was supplied to, or taken by a third party for a specific purpose that does not usually see routine data sharing with the police. Even when SWP can lawfully hold the images, the need for the Watchlist to be a proportionate policing response requires the Authorising Officer to undertake a careful assessment of an individual's privacy expectations against the policing need to locate them using LFR. The SWP LFR SOP outlines considerations for Authorising Officers at Section 6.
- V. On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow SWP personnel to consider and manage the risk of poor-quality images generating inaccurate LFR Alerts.
- VI. All Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.
- VII. The cameras used in the LFR system are of sufficient quality for the LFR system's needs.
- VIII. The LFR system is 'closed' and not connected to other SWP systems or the internet.
- IX. The LFR system is designed to assist SWP personnel locate people. The LFR system will always flag potential matches to at least one officer for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.
- X. LFR Deployments and the materials that support LFR Deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

Controls have also been implemented with regards to personal data retention to minimise the impact on the wider public and those on the Watchlist. The controls provide that:

1. where the LFR system does not generate an Alert, then a person's biometric data is immediately automatically deleted; *and*
2. the data held on the encrypted USB memory stick used to import a Watchlist is deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.
3. watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the Deployment.
4. where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 24 hours following the conclusion of the Deployment.

All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:

1. in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
2. in accordance with the SWP's complaints / conduct investigation policies.

**Deployment location privacy considerations.** Many Deployment locations will be identified as being necessary by the intelligence case supporting the prospects of locating persons at the site and/or how LFR plays a role within wider policing tactics. However, Authorising Officers must also consider the reasonable expectations of privacy the general public may have as a whole may have when traversing a public place where LFR is being considered for Deployment. Some places, and the people expected to be at some places by their nature attract greater privacy expectations than others. Authorising Officers also need to consider what measures are appropriate to identify the use of LFR when it is deployed, particularly where expectations of privacy may be greater. This is important to establishing if the proposed use for LFR, and the Deployment location itself is proportionate.

Authorising Officers should also consider if a proposed Deployment location attracts particular privacy concerns by reference to those expected to be at a particular location.

**Example:** Areas particularly focused on providing facilities or attractions aimed at children would typically attract greater privacy expectations over an area that typically sees attendance from the public more broadly. The public would not typically expect LFR to be sited outside a toy shop or school that may disproportionately see children passing the LFR system if the LFR system could be sited elsewhere. There may nevertheless be instances where the intelligence case, and the need to protect children makes it necessary and proportionate to deploy LFR to these areas. For example if it is known that wanted sex offenders are targeting those that visit the location and it not possible to locate them by siting LFR elsewhere or using other less intrusive policing tactics. If it is necessary to use LFR at the location, mitigations to reduce the privacy impact should be used wherever possible. This could include extra measures to ensure that the signage and information about the LFR Deployment is accessible to children who pass through the Zone of Recognition. The signage should be tailored to children where necessary. Where it is possible to so, and does not increase the risk to children, the time of a Deployment and configuration of a Zone of Recognition should also seek to minimise the numbers of children assessed by the LFR system.



Areas assessed as having high expectations of privacy which give the public little option to avoid the LFR area without substantial inconvenience should generally be avoided unless the following mean that the Authorising Officer is satisfied the use of LFR in the circumstances remains necessary and proportionate:

1. the importance of using LFR in that location to realise a legitimate aim supports LFR's use;
2. the lack of a viable, less intrusive alternative available for use in the circumstances;  
*and*
3. any further mitigations to reduce any impact to the wider public in so far as it is possible to do so.

**Example:** If there was a necessity and proportionality case, based on intelligence, to deploy LFR in a residential suburban area to locate a group of burglary offenders, then we understand there may be a greater expectation of privacy in this area when compared to a non-residential area. To mitigate this, depending on the circumstances we may provide additional communication about the use of LFR, for example by leafleting local residents or posting on local neighbourhood social media groups.

**Authorising Officers:** When taking a decision to deploy LFR, Authorising Officers should record the measures taken to ensure the use of LFR causes the least possible interference to the person(s) sought and others. This should include explicit reference to any particular privacy considerations that may be relevant to a Deployment location and any mitigations in place to impact the impact of the LFR Deployment. Authorising Officers should then continue to review Deployments of LFR to ensure the use case remains appropriate.

#### 4.12 Wider Human Rights Act considerations

The right to privacy is a value which protects the autonomy and human dignity of individuals by enabling them to conduct their lives in a way of their choosing. There are therefore circumstances when freedom of thought, conscience and religion (Article 9), freedom of expression (Article 10) and freedom of assembly and of association (Article 11) may be particularly relevant.

- a) *Article 9.* The clothing people wear can be an act of thought, conscience and religion and in normal circumstances, the police do not have the legal power to require a person to remove clothing (including any headdress) simply because they are passing the LFR system. Additionally, the location where people may pass the LFR system may also engage Article 9.

**Example:** The use of LFR can assist SWP to ensure public safety, including at a place of worship where the intelligence case has identified a threat to the public. A decision to place a LFR Deployment outside a place of worship or in a way that substantially impedes access to a place of worship can engage Article 9. In this context, the public safety considerations need to be balanced against the need to use LFR at that location. If the public safety policing objectives could be achieved by deploying the LFR system elsewhere, it would not be necessary to deploy LFR at the proposed location. If the threat that makes it necessary to site LFR near to a place of worship, Authorising Officers also need to determine if the infringement on Article 9 rights is disproportionate to the likely benefits of using LFR. Considerations would typically include the impact on those seeking to access a place of worship, the likely impact on the same people without LFR (being potentially impacted by other policing measures or site closures) and the benefits to safety LFR brings the public.

- b) *Article 10 and 11* have particular relevance when considering both the policing of assemblies and demonstrations and any use of LFR which may impact on an assembly or demonstration. Article 10 is especially pertinent should people have reservations about expressing themselves as a result of an LFR Deployment. Article 11 is also relevant should the use of LFR deter people from attending an assembly or demonstration at all or otherwise cause people to minimise their involvement.

**Example:** The use of LFR can assist SWP in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. In deciding the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of the LFR Deployment.

Article 10 and 11 rights must be weighed against the need to use LFR to enable an assembly that might otherwise be disrupted by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of LFR. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety. They could also include there being focus placed on ensuring the public understand the use of LFR is to help them safety undertake their assembly.

c) *Operational Duties*

The 'operational duty' was first outlined in the case of *Osman v United Kingdom*<sup>8</sup> and concerned an alleged failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights in *Osman* found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Caselaw also supports that the police are under

---

<sup>8</sup> [1999] 1 F.L.R. 193 (ECtHR)

an Osman style duty to investigate serious allegations in a timely and efficient manner in order to uphold an individual's Article 3 rights.

The Osman operational duty has particular relevance to LFR in two contexts (i) being used to locate those posing a threat to the public or themselves where a real and immediate risk to life is identified and LFR is thought to provide an appropriate response to such risk and (ii) on an Alert being generated where the need to locate that person may engage the Osman operational duty with measures being put in place should a person generating an Alert seek to evade officers.

- d) *Article 14.* This right requires that all of the rights and freedoms set out in the Human Rights Act 1998 must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and have equal access to them. Article 14 is not a stand-alone right – there is a need to show that discrimination has affected the enjoyment of one or more of the other human rights, not that the other rights have been actually breached. The use of LFR will be relevant in circumstances where demographic performance of the LFR algorithm varied to such an extent that people of a particular demographic were more or less likely to see a False Alert generated against them. As a result there are two points to consider in relation to the LFR system (i) does the LFR system's demographic differential performance vary by a particular demographic such as it results in a person suffering a discriminatory effect and (ii) if there is a different in treatment, is this capable of an objective and reasonable justification.

## 5 Equality Act 2010

- 5.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination based on different treatment on the basis of a protected characteristic. The prohibition of discrimination applies to both direct and indirect discrimination. As a public authority, SWP must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty ("PSED").
- 5.2 SWP is required to take measures to ensure that the use of LFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of the LFR system (and then, if performance varies by any particular demographic), and (b) the operational Deployment of the LFR system:

a) *The technical performance of the LFR system.*

The Court of Appeal Bridges decision makes it clear that the PSED requires SWP to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias on grounds of race or sex. To assist the public with understanding how SWP meets its PSED duties, SWP has published the SWP LFR Equality Impact Assessment. Additionally, the SWP has published a paper entitled 'South Wales Police LFR System's Accuracy and Demographic Accuracy Variance'. This explains the steps SWP has taken to understand the statistical accuracy and demographic performance of its LFR algorithm. This includes:

1. **Independent evaluation:** A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result SWP has paid

regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by SWP. SWP has then taken this further with the National Physical Laboratory (NPL) who have undertaken a scientifically underpinned evaluation of the SWP's LFR algorithm in the operational environment and published their conclusions as regards the SWP LFR algorithm's performance. SWP has then reflected the findings in the SWP LFR Documents to inform its operational practice.

2. **Ongoing assurance:** SWP LFR Documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and also offers SWP a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends. Should a concern be identified, SWP would then be in a position to explore that further and test for issues under the oversight and scrutiny of the SWP Facial Recognition Technology and Biometrics Programme Board.
3. **Independent academic evaluation:** SWP have commissioned an independent evaluation of all aspects of Facial Recognition Technology to include LFR. The evaluation will be conducted by the National Physics Laboratory and will focus of equitability particular to ethnicity, age and gender. The study is to commence in November 2021 with ongoing reviews during the life of the study being considered under the oversight and scrutiny of the SWP Facial Recognition Technology and Biometrics Programme Board.

*b) The operational Deployment of the LFR system.*

SWP LFR Documents are also responsive to the Subject, System and Environmental Factors to ensure the LFR system is suitable for its intended use and operating correctly. Subject, System and Environmental Factors including aspects such as camera configuration, camera location, lighting conditions, the distance at which people will pass the LFR system, crowd flow levels in so far as this may result in occlusion (including by reference to the height of the subjects being sought) and points relating to an individual's age and appearance have been considered carefully in SWP LFR Documents to ensure the efficacy of the LFR system and the SWP's compliance with its Equality Act 2010 duties.

By way of example, SWP LFR Documents provide that LFR Operators are trained to identify Watchlist issues with proposed images which may impact on system performance. Where the need to use an image is deemed to be necessary and proportionate, those using the LFR system have received training to maximise the LFR system's performance and to effectively consider any issues arising from the use of such images as part of the identification process.

As a result of having taken reasonable steps to understand the statistical accuracy and demographic performance of the SWP LFR system and then in light of points relating to Subject, System and Environmental Factors, and the framework of safeguards implemented

as a result, SWP has adopted a 'fail-safe' position to ensure that absent there being other lawful grounds to take policing action:

**No Engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own opinion that there is a match between the member of the public and the Watchlist image.**

This means the LFR system is not making any decision to Engage with the public, the officer is making this decision - just as officers make similar decisions to Engage with members of the public every day (without the support of LFR). The officer is best placed to make this decision, drawing on their training and policing experience.

Similarly the officer is best placed to consider the impact of any Subject, System and Environmental Factors which may have influenced the LFR system when it generated an Alert and if such factors combine to mean an Engagement with a member of the public is not appropriate in the circumstances.

**Authorising Officers:** In order to ensure that the officer is best able to make an informed decision on any Engagement, all officers who are part of an LFR Deployment are to have been briefed on the operation of the LFR system. This includes Subject, System and Environmental Factors that can impact performance. LFR Engagement Officers should also have been given training relating to unconscious bias given their key role in the Engagement decision making process.

Beyond Subject, System and Environmental factors, SWP personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of other crime fighting techniques, for example, 'stop and search'. In this respect, it is important that the use of LFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment and, where relevant, the Community Impact Assessment informs the policing plan to support the Deployment of LFR to mean SWP upholds the Public Sector Equality Duty. Compliance with the Equality Impact Assessment will then be monitored and reviewed for the duration of that Deployment.

## **6 Data Protection Act 2018**

- 6.1 SWP processes personal data for LFR 'based on law'; specifically its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate, and the policies put in place by SWP LFR Documents. The Appropriate Policy Document and other SWP LFR Documents published by the SWP as a public body allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards SWP operates to, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.
- 6.2 For the purposes of preventing crime and disorder, Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including sensitive processing, whether processed on a computer, CCTV, still images or other media. Any recorded image from a device which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR both in terms of locating those on a Watchlist but also in terms of processing biometric

information of members of the public to confirm they are not on a Watchlist. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

*“For the purposes of this Part, “the law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”*

**Authorising Officers:** Authorising Officers already need be satisfied of the necessity to use LFR to prevent crime and disorder and ensure public safety in the context of the Human Rights Act 1998. Similarly, to satisfy Section 35(5) DPA, they need to be content that the LFR system’s processing of biometric data is strictly necessary for the law enforcement purpose. The law enforcement purpose should be clearly identified and the way in which the strictly necessary standard has been met explained.

- a) Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via LFR is not used in a manner that is contrary to the identified law enforcement purpose.

**Example: alternative policing methods to prevent threats to public security:** LFR may be deployed to police a high profile well-attended public event. When considering alternatives, in this example, other measures such as extra CCTV may be considered. However they will not always be a viable less intrusive alternative in the circumstances. For example:

1. Whilst CCTV can help ensure event safety, it lacks the ability to actively Alert officers to the potential presence of individuals of interest to them.
2. It may not be practical to expect officers to recognise larger numbers of people of interest to the Police given the nature and scale of the event, the numbers of officers available to police the event and the flow rate and number of people passing the CCTV system. This is especially relevant where the importance of making such identifications supports the use of a more suitable alternative such as LFR.
3. Where LFR is thought to offer further important protection to the public as opposed to other policing methods. For example, this may apply where the law enforcement purposes for a Deployment include wider public safety considerations. These may include the need to locate those wanted by the courts. Such persons may attend such a high-profile event and, in line with the decision of the courts to require their arrest, pose a risk to the public generally.

- b) The ‘strictly necessary’ standard may be informed by the Authorising Officer considering factors including:

1. what other policing methods have been used / discounted when seeking to locate an individual(s) on the Watchlist or to provide a series of tailored security measures;
2. the importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose through the

Deployment of LFR at the proposed location with the proposed Watchlist (for example, is the Deployment intelligence-led or otherwise supported by information which confirms that LFR can be expected to get results in the circumstances being contemplated);

3. the size and scale of the planned LFR Deployment and associated Watchlist and the level of sensitive processing anticipated as a result of the LFR Deployment; *and*
4. if the law enforcement purpose which underpins the use of LFR is strictly necessary and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

**Authorising Officers:** Authorising Officers need to be satisfied that the processing satisfies one of the Schedule 8 conditions set out below and complies with the six data protection principles.

### 6.3 Schedule 8 conditions of the DPA are engaged:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk; **and**
- necessary for the purpose of preventing fraud.

**Example:** The use of LFR will assist SWP in fighting knife crime in support of its common law policing powers. LFR could be deployed to identify wanted offenders who have failed to comply with court bail relating to such offences. Used in this way, LFR would assist in the prevention, investigation, detection or prosecution of criminal offences.

LFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description to scan a crowd and try and spot an offender where positive results would otherwise be less likely and the risk of people being missed, higher. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context LFR's use may be seen as strictly necessary to support the investigation of knife crime, to enable the SWP to effectively respond to a pressing social need.

Similarly, the Schedule 8 condition of being necessary for judicial and statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe. For similar reasons, the court in the *Bridges* cases accepted the substantial public interest in the police using LFR to discharge their common law policing duties.

6.4 SWP has also undertaken a number of steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the LFR system. Particular actions are set out in the remainder of this section.

#### 6.5 Data Protection Impact Assessment:

A DPIA has been conducted to support the use of LFR in order to identify and minimise the data protection risks. Whilst the LFR DPIA will be under constant review and no later than on an annual basis, Authorising Officers authorising the use of LFR should ensure there is a DPIA in place which is sufficient for each Deployment. Specifically, consideration should to be given to:

- a. if the risks and controls remain current and sufficient for the planned use of LFR; and
- b. if the planned use for LFR poses any other risks which are capable of mitigation beyond those identified in the DPIA.

#### 6.6 Data Protection by Design:

A number of data protection controls have been designed into the LFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into LFR processing activities. The designed-in measures identified at paragraph 4.11(c) of this document, include measures to:

- a. limit the amount of personal data collected;
- b. limit the extent of personal data processing;
- c. limit the period of personal data storage.

Additionally, SWP has acted to ensure that the LFR system performs to a level where the statistical accuracy of the data being processed and fairness 'by design' is ingrained into SWP's LFR system. SWP LFR Documents and other published supporting information explain how SWP is assured that its LFR system operates with a high degree of statistical accuracy and in a way that does not lead to unjust results between demographics.

Further consideration has been given to limiting access to any personal data retained for the 31 day period. The LFR system also includes a number of physical and technical security measures including:

- a. Images are transferred onto the LFR system via a USB using an AES-CBC 256-bit full disk hardware encryption engine, that is further protected by pass-number access;
- b. The LFR system is a fully closed system with two layers of password protection to access the application. The LFR system is physically protected when in use and securely wiped following each Deployment;
- c. Role based access controls with limited user permissions are implemented on the LFR system;
- d. The LFR application is connected to mobile devices using a private access point with three levels of protection (i) specific IP addressing, (ii) password access to the access point, and



- (iii) password access to the mobile app. The mobile app has a RESTful API and will be covered by SSL;
- e. The Dashboard and RESTful API are secured with SSL and TLS by default;
- f. All connections are directed through HTTPS within a closed system;
- g. A full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*
- h. Technical issues with the LFR system are always dealt with by member of the technical staff who support the Deployment of the LFR system.

#### **6.7 Appropriate Policy Document:**

Section 42 of the DPA requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. SWP has produced this document and published it. This document allows the public to understand details of the:

- a. the data being processed by the LFR system, how often it is processed and whose data is processed;
- b. procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
- c. SWP policy for the retention and erasure of personal data for LFR processing.

#### **6.8 Data Protection Officer:**

SWP has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to LFR. The DPO is available to inform and advise the Chief Constable (as data controller) and SWP personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

## **7 General Data Protection Regulation**

7.1 As part of SWP's common law powers to protect and preserve life and property, we process special category data in accordance with the requirements of Article 9 of the UK GDPR (which is incorporated into UK law under and supplemented by Part 2 and Schedule 1 of the DPA).

7.2 The Schedule 1 DPA conditions for processing special category data require SWP to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 GDPR (relating to processing of personal data) and policies regarding the retention and erasure of such personal data.

7.3 Article 9 conditions of UK GDPR are engaged:

- explicit consent and
- substantial public interest

7.4 Section 10 DPA supplements Article 9 GDPR, requiring the following conditions of Schedule 1 to be satisfied (historical research part 1 of schedule 1 / substantial public interest part 2 of schedule 1).

7.5 Schedule 1 DPA (part 1) are engaged:

- statutory etc and research government purposes; and
- safeguarding of children or individuals of risk

7.6 Schedule 1 DPA (part 2) are engaged:

- statutory and government purposes;
- safeguarding of children

#### 7.7 Appropriate Policy Document:

Schedule 1 DPA conditions for processing special category data require SWP to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 GDPR. SWP has produced this document and published it. This document allows the public to understand details of the:

- a. the data being processed by the LFR system, how often it is processed and whose data is processed;
- b. procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Article 9 to process biometric personal data both for those on the Watchlist and those passing an LFR system;
- c. SWP policy for the retention and erasure of personal data for LFR processing.

## 8 Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a new surveillance camera code issues by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. Section 33(1) PoFA requires SWP to have regard to the Code for the use of LFR. This includes compliance with the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which SWP have regard to as follows:

| Code                                                       | SWP approach                                                                                                                                                                                                                        |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fair processing information to data subjects               | SWP processing information publically available to data subjects. It makes information relating to the LFR and data processing available via its website. The LFR Deployments are publically disclosed with supporting information. |
| Appropriate retention and disposal systems                 | The necessary systems are addressed SWP LFR Documents.                                                                                                                                                                              |
| Suitable technological and physical security measures      | These measures have been addressed by design and are also covered in SWP LFR Documents.                                                                                                                                             |
| Cameras of sufficient quality to meet the intended purpose | This requirement is addressed by the design of the LFR system.                                                                                                                                                                      |

|                                  |                                                                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitored by trained individuals | The LFR system will always flag possible matches to a trained member of SWP personnel for a decision on any further action. In this way, the LFR system works to assist SWP personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input. |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

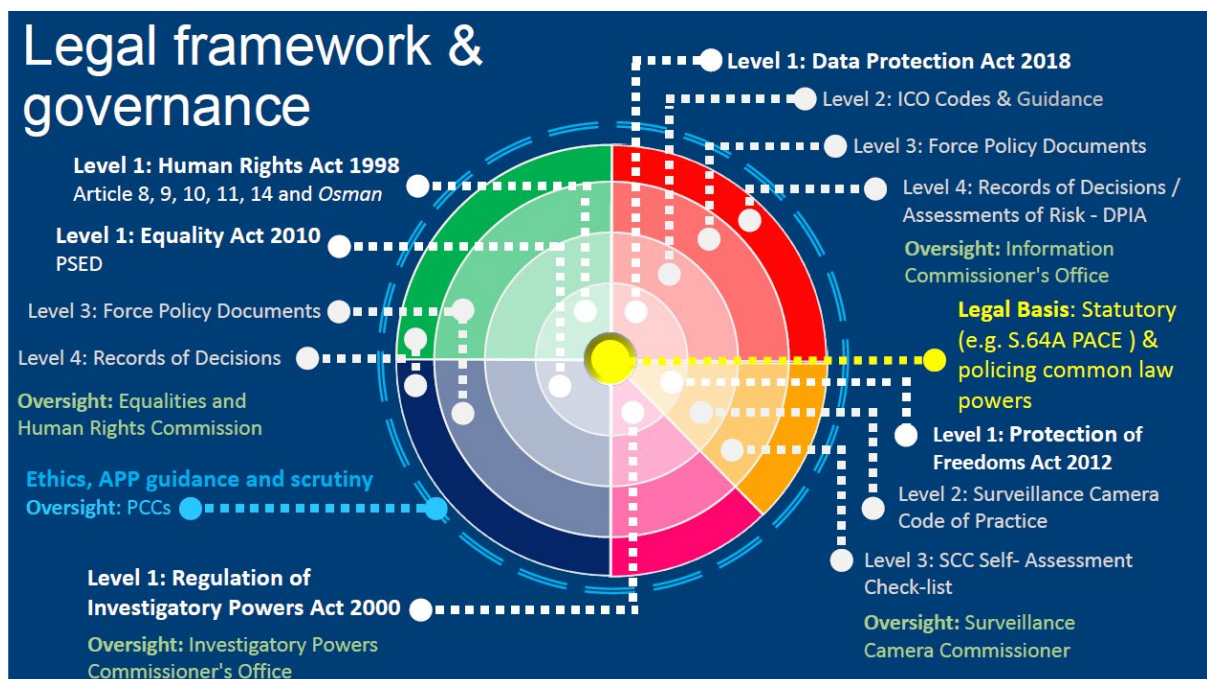
## 9 Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

- 9.1.1 public authorities are obliged to publish certain information about their activities;
- 9.1.2 members of the public are entitled to request information from public authorities.

In recognition of its FOIA duties, SWP makes significant LFR information available via its website. This includes summary information relating to LFR Deployments including the Watchlist size, the total number of Alerts, positive action and incorrect identification numbers, arrests and disposal numbers and estimates of the total number of faces seen as people passed the LFR system. SWP will also be responsive to FOIA requests.

## 10 Legal Framework and Governance Overview – summary of existing legislation and related governance regards policing’s overt use of Live Facial Recognition Technology





**SOUTH WALES POLICE**  
**POLICY DOCUMENT FOR THE OVERT DEPLOYMENT OF**  
**LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY**

|                         |                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------|
| Protective marking:     | Official                                                                             |
| Publication scheme Y/N: | No                                                                                   |
| Title:                  | Policy document for the overt deployment of Live facial recognition (LFR) technology |
| Version:                | Version 1.2                                                                          |
| Summary:                | Guidance for SWP Deployment of Live Facial Recognition Technology.                   |
| Department:             | Digital Services Division                                                            |
| Review date:            | 29/06/2023                                                                           |

**Change control:**

| Version | Date       | Authority         | Evidence of approval   | Record of change |
|---------|------------|-------------------|------------------------|------------------|
| 0.1     | 30.03.2021 | Project Lead      | Ch. Insp. Scott Lloyd  | Initial Draft    |
| 0.2     | 14.06.2021 | DSD SMT Review    | Ch. Supt Simon Belcher | Minor Amendments |
| 0.3     | 04.11.2011 | Project Oversight | Ch. Insp Scott Lloyd   | Minor Amendments |
| 0.4     | 09.11.2021 | DSD SMT Review    | Ch. Supt Simon Belcher | No Amendments    |
| 1.0     | 11.11.2021 | SRO Review        | ACC Mark Travis        | No Amendments    |
| 1.1     | 03.03.2022 | Project Oversight | Ch. Insp Scott Lloyd   | Minor Amendments |
| 1.2     | 01.05.2023 | Project Oversight | Ch. Insp Scott Lloyd   | Amendments       |

# Table of Contents

|     |                                                    |    |
|-----|----------------------------------------------------|----|
| 1   | Introduction, Aim and Scope.....                   | 3  |
| 2   | Terminology .....                                  | 5  |
| 3   | LFR Overview .....                                 | 10 |
| 4.  | Strategic Intention, Objectives and Use Case ..... | 12 |
| 5.  | Overview of LFR Deployment Processes .....         | 15 |
| 6.  | Governance, Oversight and Impact Assessments.....  | 17 |
| 7.  | Oversight Bodies and Regulatory Framework .....    | 23 |
| 8.  | Public Engagement.....                             | 24 |
| 9.  | Watchlist Considerations .....                     | 26 |
| 10. | Testing Equitability .....                         | 29 |
| 11. | Design Guidelines for LFR .....                    | 31 |
| 12. | Cameras and Camera Placement .....                 | 32 |
| 13. | Key Performance Metrics.....                       | 33 |
| 14. | LFR Guidance Summary.....                          | 34 |
| 15. | Acronyms used in LFR .....                         | 35 |

*Terms & Definitions: Capitalised terms used within this LFR Guidance Document shall have the meaning given to them in section 2 of this document unless otherwise defined.*

# 1 Introduction, Aim and Scope

## Introduction

- 1.1 Live Facial Recognition (LFR) is used by South Wales Police as a precision crime-fighting tactic to locate people who are wanted for criminal offences and helps protect the most vulnerable in our society. More detail about how LFR works and how SWP uses it can be found in section 4 (LFR Overview).
- 1.2 This LFR Guidance Document provides SWP personnel with advice on the overt use of LFR in a legally compliant and ethical manner to enable SWP to achieve legitimate policing aims.
- 1.3 SWP is also cognisant of the views and ongoing considerations of the Information Commissioner, Biometrics Commissioner, and the Surveillance Camera Commissioner and has participated in the development of national guidance and a code of practice relating to LFR and its use by UK Law Enforcement Agencies (LEA).

## Aim & Scope

- 1.4 This guidance aims to:
  - a) provide SWP personnel and members of the public with information about SWP's present strategic, operational and technology objectives for the overt use of LFR, such that its enables SWP to achieve its law enforcement purposes and is compliant with key recommendations (the Objectives); and
  - b) provide SWP personnel with guidance on the Deployment of overt LFR technology by SWP in spaces accessible to the public to meet SWP's objectives for LFR; and
  - c) establish the governance structure for the Deployment of LFR, ensuring that SWP use of LFR is appropriately governed and legally compliant; and
  - d) provide an overview of LFR technology and advise on practical issues such as camera selection and placement in order to obtain the best performance from the LFR system.

## Not in Scope

- 1.5 There are other forms of facial recognition technology (FRT) that are not subject of this guidance. This includes Retrospective Facial Recognition (RFR), which relates to non-real-time searching of images against a database. Also, not in scope is Operator Initiated Facial Recognition (OIFR) where an officer takes a picture of a subject via a mobile device and submits it for immediate search. This is still fundamentally different from LFR in that a human operator has made the decision to submit a particular Probe Image for analysis.
- 1.6 In summary, this guidance does not extend to:-
  - a) manually instigated facial recognition for retrospective searching of video / still images; or
  - b) human initiated facial search submitted from a mobile device in near real-time; or
  - c) any SWP use of third-party LFR systems, or data sharing for the purpose of facilitating the use of those systems. In such instances additional privacy considerations would

be required (e.g. additional Information Sharing Agreements and audit requirements), which are beyond the scope of this guidance; or

- d) the legal framework that is applicable to SWP's use of LFR – this is separately detailed within SWP's Legal Mandate document.

## **Additional Documents**

1.7 A number of documents are available to supplement this guidance and these include but are not limited to, the:-

- a) SWP LFR Standard Operating Procedure (SOP)
- b) SWP LFR Data Protection Impact Assessment (DPIA)
- c) SWP LFR Legal Mandate
- d) SWP LFR Appropriate Policy Documents
- e) SWP LFR Equality Impact Assessment
- f) SWP LFR Training Documents and User Guides.

## 2 Terminology

- 2.1 Within SWP and throughout SWP LFR Documents, the following terms and definitions apply in relation to Live Facial Recognition:-

### Adjudication

A human assessment of an alert generated by the Live Facial Recognition (LFR) application by an LFR engagement officer (supported, as needed by the LFR operator) to decide whether to engage further with the individual matched to a watchlist image. In undertaking the adjudication process, regard is to be paid to subject, system and environmental factors.

### Administrator

A specially trained person who has access rights to the LFR application in order to optimise and maintain its operational capability.

### Alerts

An alert is generated by the Live Facial Recognition application when a facial image from the video stream is being compared against the watchlist and returns a comparison (similarity) score above the threshold.

### True Alert

A true alert is determined when the probe image is the same as the candidate image in the watchlist.

### Confirmed True Alert

Following engagement, a confirmed true alert is determined when the engaged individual is the same as the person in the candidate image in the watchlist.

### True Recognition Rate

It is the total number of times an individual(s) on a watchlist known to have passed through the zone of recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the zone of recognition (regardless of whether an alert is generated).

This is also referred to as the true positive identification rate.

### False Alert

When it is determined by the operator that the probe image is not the same as the candidate image in the watchlist, based on adjudication without any engagement.

(The false alert rate is one of the two measures relevant to determining application accuracy).

### Confirmed False Alert

Following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist.

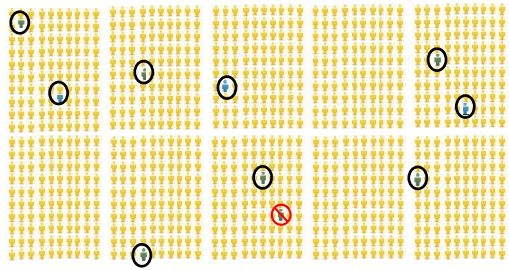
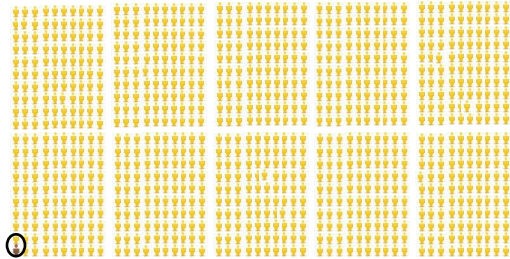
### False Alert Rate

The number of individuals that are not on the watchlist who generate a false alert or confirmed false alert, as a proportion of the total number of people who pass through the zone of recognition. This is also referred to as false positive identification rate.



### Application Accuracy

Application accuracy can be considered to consist of the combined LFR technology accuracy and the human in the loop decision-making process. Accuracy is determined by measuring two metrics, the True Recognition Rate and the False Alert Rate. This is further explained below. The example given has been simplified to demonstrate the concept, but note that the metrics have been calculated in accordance with the agreed scientific method as set out by the International Organisation for Standardisation:

|                | True Recognition Rate                                                                                                                                                                                                                                                                                                                        | False Alert Rate                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What is it?    | It is the total number of times an individual(s) on a watchlist known to have passed through the Zone of Recognition, correctly generating an alert, as a proportion of the total number of times those individuals pass through the Zone of Recognition. This is regardless of whether an alert is generated by the LFR application or not. | Is the number of individuals that are not on the watchlist who generate a False Alert or Confirmed False Alert as a proportion of the total number of people who pass through the Zone of Recognition.                                                        |
| Worked Example |  <p>The True Recognition Rate would be 90% if 10 people on the watchlist each pass the LFR system, and an Alert is generated correctly for 9 out of 10 of those people (with no alert being generated against the 10th person).</p>                        | <p>The False Alert Rate would be 0.1%, if for every 1,000 people that passed the LFR system, an Alert was generated against one person who was not on the watchlist.</p>  |

### Authorising Officer (AO)

The officer officer (usually holds the rank of Superintendent or above) who provides the authority for LFR to be used.

### Biometric Template

A digital representation of the features of the face that have been extracted from the facial image. It is these templates (and not the images themselves) that are used for searching and which constitute biometric personal data. Note that templates are proprietary to each facial recognition algorithm. New templates will need to be generated from the original images if the LFR application's algorithm is changed.

### Blue Watchlist

A watchlist comprises known persons that can be used to test system performance, for example, police officers / staff may be placed on a blue watchlist and 'seeded' into the crowd who walk through the zone of recognition during a deployment.

#### Candidate Image

Image of a person from the watchlist returned as a result of an alert.

#### Deployment

Use of an LFR application as authorised, as authorised by an AO to locate those on an LFR watchlist.

#### Deployment record

An amalgam of the LFR application, the written authority document and the LFR cancellation report. This sets out the details of a proposed deployment including – but not limited to:

- a. location
- b. dates and times
- c. deployment and watchlist rationale
- d. legal basis
- e. necessity
- f. proportionality
- g. safeguards
- h. watchlist composition
- i. authorising officer
- j. resources
- k. relevant statistics
- l. outcomes
- m. summary of any issues
- n. threshold setting

#### Engagement

An officer communicating with a member of the public as a result of an alert.

#### Environmental Factors

An external element that affects LFR application performance, such as dim lighting, glare, rain, mist.

#### Faces per frame

A configurable setting that determines the number of faces that can be analysed by the LFR application in each video frame.

#### Facial Recognition Technology (FRT)

This technology works by analysing key facial features, generating a mathematical representation of these features, and then comparing them against the mathematical representation of known faces in a database and generates possible matches. This is based on digital images (either still or from live camera feeds).

#### False Negative

Where a person on the watchlist passes through the zone of recognition but no alert is generated. There are a number of reasons false negatives occur; these include application, subject and environmental factors, and how high the threshold is set.

#### Gold Commander

Is the officer who assumes overall command and has ultimate responsibility and accountability for the Deployment. (They are responsible and accountable for the policing operation/event and determine the strategic objectives).

#### Live Facial Recognition (LFR)

LFR is a real-time deployment of facial recognition technology, which compares a live camera feed(s) of faces against a predetermined watchlist in order to locate persons of interest by generating an alert when a possible match is found.

#### LFR Engagement Officer

An officer whose role is to undertake the adjudication process following an alert, which may or may not result in that officer undertaking an engagement. These officers will also assist the public by answering questions and helping them to understand the purpose and nature of the LFR deployment.

#### LFR Operator

An officer or staff member whose primary role is operating the LFR system. They will consider alerts and, via the adjudication process, will assist LFR engagement officers in deciding whether an alert should be actioned.

#### LFR System Engineer

A person who SWP deems to have suitable technical qualifications and experience to optimise and maintain the operational capability of SWP LFR system.

#### Person(s) of Interest

A person on a watchlist

#### Possible Match

A person returned as a result of the probe and candidate image being of sufficient similarity above the threshold.

#### Probe Image

A facial image which is searched against a watchlist.

#### Recognition Time

The average time from when a face appears in the zone of recognition of the camera to when the LFR application generates an alert.

#### Retrospective Facial Recognition (RFR)

A post-event use of facial recognition technology, which compares still images of faces of unknown subjects against a reference image database in order to identify them.

#### Silver Commander

The officer who commands and coordinates the overall tactical implementation of the LFR Deployment in compliance with the strategy set by the Gold Commander. (The silver commander develops, commands and coordinates the overall tactical response of an operation, in accordance with the strategic objectives set by the gold commander).

#### Similarity Score

Is a numerical value indicating the extent of similarity between the probe and candidate image, with a higher score indicating greater points of similarity.

#### Subject Factor

A factor linked to the individual, for example, demographic factors or physical features or behaviours for example, the individual is wearing a head covering, is smoking, eating, or looking down at the time of passing the camera.

#### System Factor

A factor relating to the LFR application such as the algorithm.

#### Threshold

The configurable point at which two images being compared will result in an alert. The threshold needs to be set with care to maximise the probability of returning true alerts whilst keeping the false alert rate to an acceptable level.

#### Urgency

In the context of authorising an LFR deployment, a deployment that is related to an: Imminent threat-to-life or serious harm situation; and/or intelligence / investigative opportunity with limited time to act, where the seriousness and potential benefits support the urgency of action.

#### Watchlist

A set of known reference images against which a probe image is searched. The watchlist is normally a subset of a much larger collection of images (from the reference image database) and will have been created specifically for the LFR deployment.

#### Zone of Recognition

A three-dimensional space within the field of view of the camera and in which the imaging conditions for robust face recognition are met. In general, the zone of recognition is smaller than the field of view of the camera, so not all faces in the field of view may be in focus and not every face in the field of view is imaged with the necessary resolution for face recognition.

## 3 LFR Overview

### LFR in a Law Enforcement Context

- 3.1 Live Facial Recognition (LFR) is used by SWP as a precision crime-fighting tactic to locate people who are wanted by SWP and/or the Courts. It helps us protect the most vulnerable in our community.
- 3.2 LFR also helps us locate those on a Watchlist, by monitoring facial images of people within a Zone of Recognition. Images from specially placed cameras are searched against a Watchlist of Candidate Images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. Watchlists composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment.
- 3.3 LFR works by analysing key facial features to generate a mathematical representation of them. This representation is then compared against known faces in a database in order to identify Possible Matches against persons of interest to LEAs. Where the LFR application identifies a Possible Match, the LFR system flags an Alert to a trained member of SWP personnel who then makes a decision as to whether any further action is required. In this way, the LFR application works to assist SWP personnel to make identifications rather than acting as an autonomous machine based process devoid of user input.

### LFR and SWP

- 3.4 LFR has been trialled by SWP over a period of six years. SWP believes that LFR is a valuable precision policing tool that helps SWP to keep the public safe and to meet its common law policing duties, which include the prevention and detection of crime, the preservation of order, and bringing offenders to justice.
- 3.5 The following are illustrative examples where LFR may assist SWP with its policing purposes:-
  - a) Supporting the location and arrest of people wanted for criminal offences;
  - b) Preventing people who may cause harm from entering an area (e.g. under football banning orders);
  - c) Supporting the identification of people about whom there is intelligence to suggest that they may pose a risk of harm to themselves or others (e.g. stalkers, terrorists, missing persons, sex offenders etc.);
  - d) Supporting the use of targeted preventative policing tactics in areas where intelligence suggests violent crime may be committed or there is otherwise a need to secure an area with a precise crime fighting tool to better deter those who may pose a threat from attending.

- 3.6 Whilst appropriate use of LFR as a precision crime fighting tactic delivers clear value to UK Law Enforcement and the public in turn, it is important to recognise that the use of LFR involves biometric processing. SWP is conscious that the use of LFR has been the subject of much debate. Areas subject of particular debate and scrutiny relate to the intrusion into civil liberties and the instances of false-reporting relating to the accuracy of LFR, the potential for wide-scale monitoring through the use of LFR, and the possibility for automated decision making as a result of LFR processing.
- 3.7 It is therefore incumbent on SWP to ensure that LFR is used lawfully and responsibly for legitimate policing purposes, and in a manner that is transparent. This will help ensure that public trust and confidence is not eroded by the use of LFR.
- 3.8 In seeking to address other potential concerns, SWP has facilitated academic research led by the National Physics Laboratory, and has proactively engaged with civil liberty interest groups and South Wales Police and Crime Commissioner's Office. SWP has also commissioned the National Physical Laboratory (NPL) to undertake a ground-breaking equitability study on the use of LFR technology in an operational context to further build on the high levels of diligence already conducted on the FRT algorithm.
- 3.9 SWP has listened carefully to many parties with an interest in the use of LFR and has carefully considered what safeguards are necessary to support the use of LFR. Each Deployment must be carefully designed and have clear documented objectives. The Authorising Officer (AO) must ensure that their assessment and authorisation clearly articulates legality, necessity and proportionality. Whilst considering proportionality, the AO should address how the public benefits from the use of LFR and how this compensates for any concerns the public may have with regards to how their human rights are engaged.
- 3.10 The AO must also be satisfied that LFR Operators and LFR Engagement Officers involved with the Deployment are appropriately trained, briefed, and accountable. Also, that equipment will be used correctly, and that those involved in the Deployment mitigate against inappropriate responses to LFR application Alerts.
- 3.11 The AO must also consider how the Deployment of LFR may impact on communities as a whole, and how the rights of everyone whose image is likely to be captured by the LFR application have been considered, and what safeguards are in place to protect them.
- 3.12 SWP is not only concerned with developing and implementing precision policing tactics that protect the public as effectively as possible, but also ensuring that new tactics, such as LFR, are monitored for impact. SWP will implement a robust governance process to review the effectiveness and impact of LFR Deployments on an ongoing basis. SWP will focus on delivering transparency and will achieve this by both responding to scrutiny as well as proactively engaging and involving a range of stakeholders, including people drawn from South Wales communities as part of an ongoing process.
- 3.13 This guidance document will continue to evolve to reflect changes in legislation, regulation, technology, and accepted use.

## 4. Strategic Intention, Objectives and Use Case

4.1 LFR Deployments must be run under a Written Authority Document that complies with the following strategic intentions and operational objectives.

### Strategic Intentions

4.2 SWP will:-

- a) use overt LFR technology in a responsible way to locate offenders in accordance with SWP's common law policing powers. This includes targeting those wanted for criminal offences, those who pose a risk of harm and those wanted by the courts.
- b) comply with the common law and statutory safeguards in delivering its policing operational duties, and relies on the common law to discharge a number of its duties. LFR can assist with SWP's duties 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. This includes targeting those wanted for offences. It also includes using LFR technology to protect the public, reduce crime and help safeguard vulnerable persons.
- c) strengthen and develop LFR technology capability to protect the public, reduce serious crime, to help safeguard vulnerable persons, and to keep South Wales Safe.
- d) build public trust and confidence in the development, management and use of LFR by taking account of privacy concerns and maximising transparency; and
- e) maintain good governance through a command structure that incorporates strategic, operational and technical leads for the Deployment of LFR, with clear decision making and accountability; and
- f) ensure that the Deployment of LFR is used in compliance with all applicable legal requirements, and that it meets the oversight and regulatory framework as presently outlined in England & Wales by the Biometrics and Surveillance Camera Commissioner, the Information Commissioner and SWP LFR Documents; and
- g) transparently identify, manage and mitigate reputational and organisational risk to SWP; and
- h) be recognised as a progressive, responsible and ethical organisation.

## Operational Objectives

### 4.3 SWP will:-

- a) use LFR technology to enable SWP to discharge its common law policing powers. This includes the need to tackle our foremost operational priorities; and
- b) adopt a robust and proportionate approach in engaging and pursuing individuals identified on an LFR Watchlist, using human decision-making. Officer oversight is active and involved, with the officer retaining full control and making the decision on whether or not to take action; and
- c) engage with and provide reassurance to communities, listening and responding to concerns; and
- d) continually identify and review risks relevant to the LFR technology, mitigate those risks, and maintain a response plan should mitigation fail.

## Technological Objectives

### 4.4 SWP will:-

- a) ensure all LFR technology is fit-for-purpose and deployed effectively in line with strategic intentions and operational objectives; and
- b) provide ongoing technical oversight and evaluation into the effectiveness of the technology as a policing tactic to bear down on violent crime and other imprisonable offences; and
- c) look to technological improvements whilst keeping the SWP LFR SOPS under review. Where appropriate we will trial alternative providers of facial recognition software and hardware in parallel with our current provision. This helps to ensure that the best possible service is sought, and we are able to proactively develop improved working methodologies and accuracy. The outcomes of any parallel trial will be captured with the same key performance metrics that are gathered when deploying LFR to ensure the findings are suitable for direct comparison and analysis. All previously detailed retention periods will remain unaffected.

## Use of LFR

- 4.5 This guidance relates to the use of LFR in an overt capacity to help SWP protect the public. SWP will keep the use of LFR under review to ensure LFR continues to be used as an effective crime fighting tool.
- 4.6 LFR helps SWP use its resources more efficiently. SWP considers that LFR is better than humans at recognising persons from a large dataset (generally hundreds to low thousands) and quickly linking a Possible Match, whilst providing information that indicated why they may be of interest to SWP.
- 4.7 The use of LFR also helps minimise information sharing, as LFR offers an alternative to social media campaigns, or the sharing of information with external agencies. (It is acknowledged that considerations regards data protection should not be considered as an absolute barrier to information sharing).



- 4.8 Locations for the Deployment of LFR will be kept under strict review, with LFR being Deployed into areas where it has the greatest potential to assist SWP in discharging its operational duties. The decision to deploy LFR will always be supported by a rationale that explains why a location was selected for LFR use in accordance with the principles set out in the Legal Mandate and other SWP LFR Documents.
- 4.9 Given that LFR requires a member of SWP personnel to review every Alert in real-time for a decision as to whether any further action is required, SWP will always deploy LFR in a way that is operationally effective and allows SWP to act on any Alerts as they are generated. LFR will not be used indiscriminately.

## 5. Overview of LFR Deployment Processes

### End-to-End Process

5.1 The end-to-end process of an LFR Deployment can be summarised as follows:-

- a) LFR law enforcement purpose identified, safeguards considered, Deployment authorised, and Watchlist selected;
- b) Notification of Deployment, and signage deployed;
- c) As subjects pass an LFR camera, their faces are detected, and if the image quality is sufficient, they are compared against a Watchlist;
- d) If a Possible Match is found in a Watchlist, the LFR application generates an Alert and both the detected face from the video and the Possible Match image from the Watchlist are presented to the LFR Operator / LFR Engagement Officer for human review;
- e) The LFR Operator / LFR Engagement Officer will consider the Alert, noting the System, Subject and Environmental Factors, and together with the benefit of their experience and training, they will determine whether further action is required and whether the person is Engaged;
- f) Cancellation of authority for the LFR Deployment and post-Deployment evaluation.

5.2 SWP LFR SOP provides a greater level of detail about the processes involved in the Deployment of LFR by SWP. A flowchart summarising LFR Deployment can be found in Section 13 of this document.

### Key Points

- a) LFR uses images from people within the LFR Zone of Recognition. No individual is 'targeted' any more than another unless they are on a Watchlist;
- b) The selection and placement of cameras is a vital consideration to ensure proper coverage of the desired area;
- c) The quality and resolution of images (both those in the Watchlist and those from the video cameras) are of vital importance and must be carefully considered;
- d) The inclusion of persons on a Watchlist needs to be justified based on the principles of necessity and proportionality.
- e) It is important to balance the objectives of the operation with the size of the Watchlist and the available resource to respond to Alerts. If the objectives are too broad and/or the Watchlist is too large, the amount of resource required to respond to Alerts may be prohibitively high.

## Policing LFR Deployments Effectively

- 5.3 There must be sufficient appropriately trained resource deployed so as to be able to respond to Alerts. This is important in order to ensure that the LFR application, and the data processed by it, is being effectively used.
- 5.4 The volume of people expected to pass through the LFR Zone of Recognition will influence the rate of False Negatives, False Alerts, Recognition Time, and the probability of people from the Watchlist being observed by the camera (i.e occlusion) and their likely presence are all matters that must be taken into account when deciding what resources should be available.
- 5.5 It is also vital that SWP is transparent in its use of LFR under this guidance. As well as using signage, the provision of sufficient policing resource will allow officers to answer questions that the public may have.

## 6. Governance, Oversight and Impact Assessments

6.1 Following consultation the following stipulations have been proposed and accepted by SWP:-

- a) The overall benefits to the public must be balanced with public confidence of our use of LFR;
- b) It can be evidenced that the technology itself will not result in unacceptable gender or racial accuracy variance into policing operations;
- c) Each Deployment must be appropriately assessed and authorised, demonstrating both necessary and proportionate for a specific policing purpose;
- d) LFR Operators are trained to understand the risks associated with use of the LFR application, including how potential injustices may be caused through inappropriate responses, and that they are accountable for their actions;
- e) SWP, will develop and maintain robust governance and oversight arrangements that balance the technological benefits of LFR with their potential intrusiveness. These arrangements will meet the Home Office Biometric Strategy's requirement for transparency, whilst taking into account guidance from the Surveillance Camera and Biometric Commissioner. The arrangements will also focus on implementing a transparent and visible internal inspection, audit, and compliance enforcement regime.

### Governance Framework

6.2 SWP LFR Documents address the stipulations detailed above. Governance and oversight of the use of the technology is approached in three stages, as follows:-

- a) Pre-Deployment;
- b) Operational Deployment;
- c) Post-Deployment.

### Pre-Deployment

6.3 Authority to Deploy LFR is an operational one, where SWP Authorising Officer (AO) rank is set at Superintendent. In exceptional cases of urgency, an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR.

6.4 Where an officer below the rank of Superintendent provides the authority, a Superintendent must be informed as soon as practicable. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority where they believe necessary, or direct that it must stop.

- 6.5 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an SWP officer of NPCC rank<sup>1</sup> (or police staff equivalent) must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby issues are taken into account as much as possible. This affords NPCC the opportunity to scrutinise the Deployment and to ask the AO to consider what mitigation is required to address concerns at hand.
- 6.6 The AO must notify the SWP Police and Crime Commissioner (or designated staff member) prior to any deployment.
- 6.7 SWP Ethics Committee are an independent source of advice. Their terms of reference include the provision of advice and independent oversight of SWP on ethical matters, and the promotion of ethical considerations within a legal and regulatory framework.

---

<sup>1</sup> NPCC – ‘NPCC rank’ denotes an officer holding the rank of ACC or above.

- 6.8 A number of specific SWP documents and records need to be completed in support of each Deployment. These are set out below:-

| SWP LFR Deployment Specific Documents and Records |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LFR Application                                   | Sets out the details of a proposed Deployment including location, dates/times, legitimate aim, legal basis, necessity, proportionality, safeguards, Watchlist composition, and resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Written Authority Document                        | <p>The AO's written authority provides a decision making audit trail demonstrating how the AO has considered the legality, necessity and proportionality of the Deployment of LFR, the safeguards that apply and the alternatives that were considered but deemed to be less viable to realise the policing purpose.</p> <p>The written authority also details the arrangements that have been made to manage the retention and/or disposal of any personal data obtained as a result of the LFR Deployment.</p> <p>The written approval must be retained in accordance with MOPI and other relevant legislation or policy and be made available for independent inspection and review as required.</p> |
| LFR Deployment Record                             | Records details of where and when a Deployment was carried out, what resources were used, relevant statistics, outcomes and summary of any issues.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Assessments                                       | <p>These include the Community Impact Assessment, the Equality Impact Assessment, the Data Protection Impact Assessment, and the Surveillance Camera Commissioner's Self-Assessment.</p> <p>These documents need to be considered by the decision-maker when authoring a Deployment to ensure they are sufficient to address the issues arising from the proposed Deployment.</p> <p>The decision-maker must ensure that issues have been adequately identified, documented, and mitigated by way of safeguards such that the Deployment is not only necessary, but also proportionate to the policing purpose.</p>                                                                                     |
| Deployment Logs                                   | Logs completed in the planning and execution of an LFR Deployment. For example, logs completed by the Gold and Silver Commanders, LFR Operators and LFR Engagement Officers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

6.8 Several other specific SWP documents pertaining to each SWP LFR Deployment have been completed centrally. These are set out below:-

| SWP LFR Documents and Records                      |                                                                                                                                                                                              |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SWP Data Processing – Appropriate Policy Documents | SWP policy on the processing of data pursuant to the Data Protecting Act 2018 and UK General Data Protection Regulation relating to LFR.                                                     |
| SWP Legal Mandate                                  | Outlines the legal considerations to be addressed in order to use LFR.                                                                                                                       |
| SWP Training Materials                             | Provides the necessary training to ensure those involved in authorising and deploying LFR are familiar and implement the considerations relevant to its lawful, ethical and appropriate use. |

## Operational Deployment

- 6.9 Arrangements must be made to accurately record and log the dates, times and location of the Deployment.
- 6.10 The Silver Commander must ensure that arrangements are made to keep the use of LFR under review throughout the duration of the Deployment. The Silver Commander needs to be content:-
- a) that the use of the LFR remains necessary and proportionate for the policing purposes identified in the Written Authority Document; and
  - b) that the safeguards identified in the written approval remain effective; and
  - c) that the level of officer support committed to the Deployment is enabling Alerts to be responded to effectively; and
  - d) that the Subject, System and Environmental Factors are such that the use of the LFR application remains effective for realising the policing purpose identified in the written approval.
- 6.11 Circumstances may arise that mean that there is a need to curtail or postpone the Deployment. Examples may include occlusion resulting in those sought not being presented to the camera in cases of high crowd flow, adverse weather / lighting conditions or operational events changing the resources needed in the area. The Silver Commander must be empowered and have absolute discretion to suspend or terminate the Deployment. Further details are provided within the LFR SOP.
- 6.12 In any event the Silver Commander must conduct and record a review of the activity at suitable intervals during the Deployment. The timing and frequency of reviews is determined by the Silver Commander. A suitable period should be determined in the context of the Deployment. This review should address the continued legality, necessity and proportionality of the Deployment, as well as providing some analysis on LFR application performance and the Engagements undertaken.

## Post-Deployment

- 6.13 The use of LFR should be subject to debrief and review. This will help ensure that future Deployments reflect learning identified from each Deployment, and that the use of LFR remains an effective and proportionate policing tool. The structure and form of each review should aim to achieve a degree of independence from the Gold Commander and address the efficiency and efficacy of the Deployment.
- 6.14 Each Deployment should be subject to an authority cancellation, once no longer required. The LFR Deployment Record is submitted to the AO (this may be the same person as the Silver Commander) to ensure that appropriately senior oversight is maintained. Such reports should typically be produced and submitted within 31 days.
- 6.15 The outcome of LFR Deployments are subject to evaluation, which in turn should feed into oversight and scrutiny processes.
- 6.16 Post-Deployment, SWP must ensure that the processing of any personal data associated with LFR is conducted in a lawful way in compliance with SWP LFR documents. This includes that:-



- a) where the LFR system does not generate an Alert that a person's biometric data is immediately automatically deleted; and
- b) the data held on any encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours, following the conclusion of the Deployment.

6.17 Where the LFR system generates an Alert all personal data is deleted as soon as practicable and in any case within 24 hours.

6.18 All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-

- a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
- b) in accordance with SWP's complaints / conduct investigation policies.

## 7. Oversight Bodies and Regulatory Framework

- 7.1 Within SWP, the senior internal oversight body for LFR is SWP FRT & Biometrics Programme board, which in-turn answers to DSD Gold Board. In addition, The SWP commissioner's office also provide an external oversight and scrutiny perspective.
- 7.2 SWP LFR Legal Mandate sets out the legal framework for SWP use of LFR technology, whilst SWP LFR Policy Document and SWP LFR SOP support implementation.
- 7.3 Nationally, the 'NPCC Facial Recognition Technology Board' provides oversight for the operational uses of facial recognition within UK Law Enforcement.
- 7.4 Further oversight opportunities may arise in relation to the 'Joint National Biometric Strategic Board'. This is co-chaired by the NPCC and the Home Office Data and Identity Department, and involves representatives of the Information Commissioners Office, the Surveillance Camera Commissioner, and the Biometric Commissioner. More detail on these roles:-

- a) Surveillance Camera Commissioner (SCC); The role of the Surveillance Camera

Commissioner is to encourage compliance with the surveillance camera code of practice, review how the code is working, provide advice to ministers on whether or not the code required amendment.

Any SWP LFR system will need to comply with this Code and the twelve guiding principles. This guidance document seeks to apply those principles.

See [www.gov.uk/government/organisations/surveillance-camera-commissioner](http://www.gov.uk/government/organisations/surveillance-camera-commissioner);

- b) Biometrics Commissioner (BC); The Commissioner is independent of Government and aims to keep the police use and retention of biometric data under review. The Commissioner makes decisions on applications made by the police to retain DNA profiles and fingerprints, and reviews national security determinations that are made or renewed by the Police in connection with the retention of DNA profiles and fingerprints. The Commissioner also reports to the Home Secretary about the carrying out of their functions.

See: [www.gov.uk/government/organisations/biometrics-commissioner](http://www.gov.uk/government/organisations/biometrics-commissioner);

- c) Information Commissioner's Office (ICO); The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Protection Impact Assessment must comply with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 and should be shared with the ICO.

See [www.gov.uk/government/organisations/information-commissioners-office](http://www.gov.uk/government/organisations/information-commissioners-office).

## 8. Public Engagement

- 8.1 Public engagement must be supported by the use of online resources available to the public, which should be underpinned by a press and media strategy giving advance notice of Deployments. At and around the location of Deployments, notices providing information, including details of the Privacy Notice, should be distributed and feedback via email should be sought.
- 8.2 Operational briefings delivered to officers and stakeholders prior to Deployments should promote openness with the public and transparency about the use of LFR. Officers should be encouraged to engage with the public to increase awareness of how LFR helps keep the public safe and how it helps bring offenders to justice. It is also helpful for officers to be in possession of information leaflets that can be handed out to the public. Such information leaflets should deliver important key messages aimed at promoting trust and confidence through improved understanding.
- 8.3 Key stakeholders, including the PCC's Office, may be invited to observe the planning and Deployment of LFR.

### In Advance of Deployments

- 8.4 In advance of Deployments ensure that:-

- a) LFR Deployments are notified to the public using SWP website and other appropriate communication channels (including social media); and
- b) LFR awareness raising measures (e.g. signs and/or leaflets) are prepared to support LFR Deployment in line with SWP LFR SOP; and
- c) literature is prepared for persons who may be Engaged (to include information outlined within a privacy notice); and
- d) Officers are briefed on their powers and the limits thereof. In particular, it must be made clear that there is no power to require an individual's cooperation in having their image captured, unless either the threshold for arrest has been reached, or an Inspector or above has authorised the exercise of the power under section 60AA of the Criminal Justice and Public Order Act 1994 for a Constable in uniform to compel a person to remove anything that conceals their identity; and
- e) external engagement is considered in discussion with SWP LFR team. It may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity.

## During Deployments

### 8.5 During Deployments ensure that:-

- a) awareness raising measures are used in line with the SWP LFR SOP to ensure that the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed; and
- b) notices with a brief explanation and reference to SWP website are available to hand out to the public on request; and
- c) information is offered to persons Engaged by officers in accordance with the policy referred to above.

## After Deployments

### 8.6 After Deployments ensure that:-

- a) information about the Deployment, including location, time, date, number of Alerts, engagements, arrests, and any other information considered helpful and suitable for disclosure, is published on SWP website. Care must be taken to ensure that no personal data is published;
- b) external engagement is considered in discussion with SWP LFR team. Again, it may be appropriate to pursue engagement opportunities with a number of stakeholders, including local authorities, and public consultative or ethical review bodies. It is important that engagement is coordinated and so the LFR team must be consulted prior to this kind of activity; and
- c) engagement with representatives from the Information Commissioners Office will be ongoing.

## 9. Watchlist Considerations

### Image Quality

- 9.1 The performance of the LFR system is heavily dependent on the quality of the images in the Watchlist. The best images are those that follow a custody or passport style image that conforms to the NPIA 'Police Standard for Still Digital Image Capture and Data Interchange of facial/Mugshot and Scar, Mark & Tattoo Images (full frontal face, neutral expression, uniform lighting and plain background)'. Further detail is included within the embedded PDF:



NPIA Standard Still  
Digital Images.pdf

- 9.2 Where multiple images of a subject are available, consideration should be given to including these in the Watchlist where it is advised that they will improve the likelihood of locating those of interest to SWP.

### Compiling the Watchlist

- 9.3 SWP Legal Mandate provides commentary on the legal considerations relevant to compiling a Watchlist in a lawful way. This means that we ensure we hold the Watchlist images lawfully, that their inclusion is necessary and proportionate, and that it meets the identified policing purposes.
- 9.4 Key points include ensuring the Watchlist is limited to the size needed to meet the policing purposes identified, and taking reasonable steps to be sure that the image used should accurately identify the individual being considered for inclusion on the Watchlist. SWP LFR SOP provides practical guidance on how to follow SWP LFR Documents, including SWP Legal Mandate.
- 9.5 The size of the Watchlist is relevant to the level of resource that should be available to a Deployment. There must be sufficient resource available to manage the Alerts generated by the LFR application.

- 9.6 As explained in section 3 (LFR Overview), Watchlists composition is normally restricted to individuals suspected to be in the proximity of an area, and therefore where there is some possibility or likelihood of an individual passing through an LFR Deployment. How great that likelihood needs to be will vary between cases for inclusion, but in any case should be considered against a number of factors. This means that an AO may deem it necessary and proportionate to authorise the inclusion of people to be included in a Watchlist, even though there may not be specific intelligence to say where in SWP they might be found. Factors for consideration in this respect include:-
- a) Severity of 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 that they are wanted for a serious offence;
  - b) Risk; The level of risk associated with an individual or the offence type sought, 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 as well as informing the scope and nature of the Watchlist. Areas around transport hubs have a lot of people transiting from place to place.

### Governing the Watchlist

- 9.7 The systems used to generate the Watchlist are protected by role specific access control measures, and those using them are supported by role-specific training. This includes familiarisation with data protection principles.
- 9.8 SWP LFR Documents provide measures to ensure that the Watchlist is lawfully compiled, current, is not retained beyond its purpose, and is only used for its LFR purpose.

### Addressing Disproportionality

- 9.9 SWP does not create or retain a breakdown of race, gender or any other protected characteristic<sup>2</sup> of persons on a Watchlist. This mirrors the approach taken with the majority of policing tools used by SWP. The exception here is for inclusion of under 18's and under 13's as previously detailed.
- 9.10 The Deployment of LFR is driven by SWP policing priorities, intelligence-led assessments, both of which determine locality and the policing purpose. It is then the locality and policing purpose that determines the composition of the Watchlist. The individuals found on a Watchlist are there because there is a policing need to locate them, there are realistic prospects of doing so, and that need fits with the policing purpose driving the LFR Deployment.
- 9.11 The routine retention of data relating to protected characteristics would mean SWP holding and processing data in circumstances where it does not have a policing need to do so. In essence, holding the data would not alter the intelligence case or change the policing need to locate individuals placed on a Watchlist.

---

<sup>2</sup> As defined in Section 4 of the Equality Act 2010.

- 9.12 SWP recognises the need to ensure that the systems and processes it relies upon are not inherently biased, and in this context that they do not disadvantage individuals based on protected characteristics. Regular tests are carried out using police officers and staff volunteers who are 'seeded' into a 'Blue Watchlist'. The volunteers walk through the Zone of Recognition at the start of a Deployment to measure the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated.
- 9.13 SWP also carries out academic equitability testing of the LFR system when necessary – such tests, including with the National Physical Laboratory have been documented. The necessity and frequency is determined by factors that could affect performance, including the introduction of new and upgraded equipment, software or algorithms.
- 9.14 When equitability tests are conducted, no biometric data belonging to members of the public is retained for the purpose of the tests. As part of these tests, a human operator monitors and records perceived gender, ethnicity, age and any other relevant protected characteristics, of persons passing through the Zone of Recognition during an LFR Deployment.
- 9.15 SWP has a number of measures to guard against a System Factor (system bias) affecting the generation of Alerts. For example, being more likely to generate False Alerts based on individuals sharing the same perceived ethnicity or gender. These measures include that:-
- a) those involved in an LFR Deployment monitor Alerts, Subject Factors, System Factors and environmental Factors throughout the Deployment. Should concerns arise that the LFR system is not performing correctly, the Silver commander will halt the Deployment where necessary; and
  - b) for the purpose of facilitating post-Deployment reviews, Alerts are retained for up to 24 hours. It provides further opportunity to consider the Subject, System and Environmental Factors, Alert reliability, and the effectiveness of the safeguards in place for the Deployment, including the reviews undertaken by Silver and Gold during the Deployment; and
  - c) in the event post-Deployment reviews identify an area of concern, SWP may undertake further equitability testing where this appears necessary.

## 10. Testing Equitability

- 10.1 In August 2021 SWP was awarded Home Office Science, Technology, Analysis & Research (STAR) funding to undertake testing of the accuracy and equitability of FRT in an operational environment for LFR, OIFR and RFR.
- 10.2 In collaboration with the Metropolitan Police (MPS), this work was awarded to the National Physical Laboratory (NPL) at the end of 2021. The NPL is a prestigious world-leading centre of excellence that provides cutting-edge measurement science, engineering and technology to underpin prosperity and quality of life in the UK. In order to deliver on the objectives of the research, it was necessary to use LFR in the operational use cases of UK Policing. Data collection for the evaluation took place in July and August alongside five operational deployments of LFR, four in London and one in Cardiff.
- 10.3 A cohort of volunteers were selected to take part in the study who were of varying age, gender and race, the volunteers were seeded into the crowd passing the LFR System at each Deployment so as to appear in the LFR video footage.
- 10.4 The data was then evaluated 'post event' with a balanced Watchlist and mated facial photographs taken of the volunteers in a variety of settings to realistically replicate the use cases for LFR, RFR and OIFR.
- 10.5 The full results are presented in the National Physical Laboratory's commissioned report 'Facial Recognition Technology in Law Enforcement Equitability Study'.

### ***What does this study tell us about accuracy of SWP's FRT?***

- 10.6 The NPL report gives us an impartial, scientifically underpinned, evidence-based robust analysis of the performance of SWP's FRT System in operational conditions in terms of (i) accuracy and (ii) equitability (bias) related to subject demographics.
- 10.7 In summarising LFR operational performance, NPL have provided performance figures for two different Watchlist sizes: (i) a Watchlist of 10,000 reference images, which is broadly in line with those used on the MPS' LFR operational deployments to date and (ii) a watchlist of 1000 reference images a size more typical for SWP LFR deployments.
- 10.8 The performance figures use industry standard measures; (i) True-Positive Identification Rate (TPIR) (also known as True Recognition Rate)– the rate of successful recognition when subjects on the Watchlist pass through the Zone of Recognition (ii) False-Positive Identification Rate (FPIR) (also known as False Alert Rate) – the rate of incorrect recognition (i.e., false positives or false alerts) when subjects not on the Watchlist pass through the Zone of Recognition
- 10.9 The table below shows the results of combined data from all five deployments:

| Watchlist size 10000 |                   |                          | Watchlist size 1000 |                   |                            |
|----------------------|-------------------|--------------------------|---------------------|-------------------|----------------------------|
| Metric               | Threshold Setting | Result                   | Metric              | Threshold Setting | Result                     |
| TPIR                 | 0.60              | = 89 %                   | TPIR                | 0.60              | = 89 %                     |
| FPIR                 | 0.60              | ≈ 0.017 %<br>(1 in 6000) | FPIR                | 0.60              | ≈ 0.002 %<br>(1 in 60,000) |



***Did the study find any differences in SWP's FRT?***

- 10.10 In relation to LFR, NPL found that at a Threshold of 0.60, any differences in TPIR by gender, by race, or by race/gender combined were not statistically significant. This means that the systems performance is not biased towards any race or gender. The study has shown that at Thresholds of 0.60, 0.62 and 0.64 the number of subjects with a false positive is very small and there is no statistically significant imbalance between demographics.
- 10.11 The study has shown that at a face match Threshold of 0.64 or higher there was no false positive identifications. Thus, at this Threshold the FPIR is identical for race, age and gender.
- 10.12 In relation to age, the NPL found that at a Threshold of 0.62 the observed differences in TPIR were not statistically significant. At a Threshold of 0.60, the observed variation in TPIR did show statistical significance with TPIR improving with subject age. This means that the system is slightly more likely to locate those sought as they age, but not more likely to inconvenience those of younger age, as the FPIR is found to be equitable between gender, race, and age. There is no statistically significant imbalance between demographics. In relation to trying to locate those of younger age, the NPL recognised;
- “.....the lower performance of the under 20s is therefore assessed to be due to both demographic and environmental factors, these being a combination of subject age and as a result subject height, and crowdedness in the zone of recognition.....”
- 10.13 Where SWP is particularly seeking to locate those of younger age and whom maybe of a shorter stature, consideration should be given of how busy the area is. The risk that subjects may be shielded from the camera by a taller person walking in front of them and blocking the camera's view must be taken in to account. Therefore, deployment locations and camera positioning should form part of the technical optimisation process.
- 10.14 Reflective of the need for continuous improvement, SWP will continue to monitor its FRT performance, in terms of both overall system accuracy and demographic differential performance going forward.

## 11. Design Guidelines for LFR

- 11.1 A new international standard (ISO IEC 30137-1: 'Use of biometrics with video surveillance systems, Part 1: System design and specification') was published in May 2019. See [www.iso.org/standard/64935.html](http://www.iso.org/standard/64935.html).
- 11.2 ISO IEC 30137-1 provides additional detail covering technical aspects of specifying and implementing a facial recognition system for use with video cameras, including camera selection and placement, adjustment of detection and matching Thresholds, Watchlist management, and the role of the LFR Operator. It is strongly recommended that forces considering the use of LFR use the guidance to supplement the technical overview provided here. SWP has done this.
- 11.3 SWP LFR processes and associated guidance has been developed so as to provide for a reliable means of locating individuals using LFR with high definition CCTV cameras (2MP and above). For a recognition system to deliver the desired results, all components need to be optimised and interoperate correctly. These system components include the hardware, the software, the LFR Operator, and associated policing resources on the ground.
- 11.4 A system using facial recognition will consist of many components. Those components that do not directly relate to the successful use of facial recognition are not considered in this guidance. Directly relevant components include:-
  - a) the Cameras, including cabling, and their placement; and
  - b) the environment in which the cameras operate; and
  - c) the database of reference images and associated meta data, often referred to as the Watchlist; and
  - d) the facial recognition software that detects faces in the footage, converts the facial images into Templates, compares these against the Watchlist and provides information on the results of the comparison (generally in the form of an Alert or a numerical score) to an LFR Operator; and
  - e) the LFR Operator and LFR Engagement Officer who assess Alerts and determine the appropriate course of action; and
  - f) having sufficient officer resource to support the Deployment.

## 12. Cameras and Camera Placement

- 12.1 Cameras must be selected so that the image resolution, frame-rate, field-of-view and low-level light performance can provide images of sufficient quality for use in the facial recognition application. Current FR systems typically require a facial image with between 20 and 100 pixels between the centres of the subject's eyes (Inter-Eye Distance or IED). The FR vendor should advise on specific requirements for their system.
- 12.2 Unless the environment is well controlled, cameras must be capable of operating at Wide Dynamic Range in order to generate high quality images under a variety of lighting conditions.
- 12.3 Cameras should ideally be positioned to capture faces as close as possible to the 'face-on' condition, similar to a passport image. This typically requires the cameras to be much lower than is normally the case for existing CCTV. Camera placement and angle should be further considered where those sought may be more likely to be occluded in a busy crowd in order to maximise the prospects of location.
- 12.4 Ideally the environment should be managed such that every face is evenly illuminated. Highly directional lighting, for example strong sunlight, should be avoided, which may require consideration of how the lighting will change throughout the day.
- 12.5 In general, the Zone of Recognition will be smaller than the field of view of the camera; for example, not all faces in the field of view may be in focus and not every face in the field of view will be imaged with the minimum necessary Inter-Eye Distance (IED).
- 12.6 A typical 2MP camera will provide sufficient resolution for LFR to work on a maximum of 3 to 4 people side by side. Therefore, consideration needs to be given to camera location and the physical environment. For example, looking for opportunities to funnel or restrict the movement of people within the Zone of Recognition. However, if the flow is reduced beyond a certain level, individuals may be grouped very close together, occluding or partly occluding the faces of people (people behind people).
- 12.8 Detection and processing of faces is an intensive task for a computer system. The supplier of LFR software should provide guidance on hardware requirements and the number of faces that can be simultaneously processed from within a single frame. If the system is set to process too many faces, this will potentially result in delays to the LFR system response. It may also result in missed Alerts due to 'dropped frames' where the software skips some of the video footage in an attempt to catch up.

## 13. Key Performance Metrics

- 13.1 This section covers some of the key performance metrics that should be gathered when deploying LFR. It outlines the minimum requirements and so additional metric or indicators may well be relevant and suitable for collation and analysis. There are two key metrics that determine the 'accuracy' of an LFR system. These are detailed in the below paragraphs.

### True Recognition Rate

- 13.2 The number of times when individuals on a watchlist are known to have passed through the zone of recognition and the LFR system correctly generated an alert, as a proportion of the total number of times when these individuals passed through the zone of recognition (regardless of whether an alert is generated).
- 13.3 This metric can only be generated by 'seeding' known subjects (for example police officers or staff) into a Blue Watchlist and measuring the number of times those subjects are present in the Zone of Recognition against the number of Alerts generated. Users of FR systems (and vendors) must not focus so closely on maximising this metric, that they increase the False Alert Rate to inappropriate levels.

### False Alert Rate FAR

- 13.4 There are two types of False Alert Rate (FAR) measurements. The first is the System FAR, which is the number of False Alerts generated as a proportion of the total number of subjects processed by the LFR application. The second is the Operational FAR, which is calculated in the same way, but is measured after the LFR Operator has reviewed the output from the LFR application, and dismissed LFR application Alerts assessed by the LFR Operator as false.
- 13.5 All of the TRR and FAR metrics should be recorded and reported. Operational experience to date suggests that in most scenarios the FAR should be 0.1% or less (i.e. less than 1 in 1000). It should be noted that the FAR is greatly affected by the number of subjects processed by the LFR application, and to a lesser extent, the size of the Watchlist. This is a key reason why the number of persons included on the Watchlist needs to be kept as small as possible, whilst still meeting operational objectives.
- 13.6 It should be also be noted that the configurable Threshold (the point at which two images being compared will result in an Alert) will have a direct impact on the TRR and FAR. The Threshold needs to be set with care so as to maximise the probability of returning correct Possible Matches, whilst keeping the number of False Alerts to acceptable levels.

### Recognition Time

- 13.7 A third important metric is the Recognition Time (RT). Note that the actual amount of time taken to act on an Alert will always be longer than the RT as additional time is needed for the LFR Operator to assess the Alert and to pass to an LFR Engagement Officer to then make a final decision on whether to Engage or not.
- 13.8 The RT must be sufficiently small that an effective response to an Alert is possible before the subject has moved too far from the point where the initial Alert occurred. High resolution

video cameras with multiple faces in each frame will require significant processing power if the RT is to be fast enough to enable a real-time response.

## 14. LFR Guidance Summary

- 14.1 This guidance relates to the operational use of LFR, and the governance and oversight regimes necessary to support Deployment.
- 14.2 It is strongly advised that officers and staff adhere to the guidance as this will help ensure that SWP use of LFR successfully and lawfully serves the public whilst providing necessary safeguards. It is also important to maintaining the trust and confidence of the public as well as our partners and other stakeholders.
- 14.3 It is recognised circumstances may arise where for valid reasons, a decision is taken that it is necessary to things slightly outside of this guidance. This guidance will no doubt evolve as technology changes and improves, and as learning influences what is recognised as good practice. Where decisions are taken that are at odds with some aspects of this guidance, it is essential these decisions are fully documented, together with detailed rationale, and that the relevant decision-making features within debrief and evaluation processes.

## 15. Acronyms used in LFR

|       |                                                    |
|-------|----------------------------------------------------|
| AO    | Authorising Officer                                |
| BC    | Biometrics Commissioner                            |
| CCTV  | Closed Circuit Television                          |
| CIA   | Community Impact Assessment                        |
| DPA   | Data Protection Act 2018                           |
| DPIA  | Data Protection Impact Assessment                  |
| EIA   | Equality Impact Assessment                         |
| FAR   | False Alert Rate                                   |
| FR    | Facial Recognition                                 |
| FoIA  | Freedom of Information Act                         |
| HRA   | Human Rights Act 1998                              |
| ICO   | Information Commissioner's Office                  |
| ISO   | International Standards Organisation               |
| LEA   | Law Enforcement Agency                             |
| LFR   | Live Facial Recognition                            |
| MOPI  | Management of Police Information                   |
| SWP   | South Wales Police                                 |
| NPCC  | National Police Chiefs' Council                    |
| NPL   | National Physics Laboratory                        |
| RT    | Recognition Time                                   |
| SCC   | Surveillance Camera Commissioner                   |
| SCCSA | Surveillance Camera Commissioner's Self-Assessment |
| SOP   | Standard Operating Procedure                       |
| TRR   | True Recognition Rate                              |
| UK    | United Kingdom                                     |

|     |                            |
|-----|----------------------------|
| USB | Universal Serial Bus       |
| VSS | Video Surveillance System  |
| WAD | Written Authority Document |
| ZoR | Zone of Recognition        |



## **STANDARD OPERATING PROCEDURE (SOP)** **FOR THE OVERT DEPLOYMENT OF** **LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY**

|                         |                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Protective marking:     | Official                                                                                                                 |
| Publication scheme Y/N: | No                                                                                                                       |
| Title:                  | Standard Operating Procedure for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology            |
| Version:                | Version 1.2                                                                                                              |
| Summary:                | Establishes procedures for the Deployment of Live Facial Recognition (LFR) technology in support of policing operations. |
| Department:             | Digital Services Division                                                                                                |
| Review date:            | 01/05/2023                                                                                                               |

| Version | Date       | Authority         | Evidence of approval   | Record of change |
|---------|------------|-------------------|------------------------|------------------|
| 0.1     | 18.06.2021 | Project Lead      | Ch. Insp Scott Lloyd   | Initial Draft    |
| 0.2     | 14.06.2021 | DSD SMT Review    | Ch. Supt Simon Belcher | No Amendments    |
| 0.3     | 04.11.2021 | Project Oversight | Ch. Insp Scott Lloyd   | Minor Amendments |
| 0.4     | 09.11.2021 | DSD SMT Review    | Ch. Supt Simon Belcher | Minor Amendments |
| 1.0     | 11.11.2021 | SRO Review        | ACC Mark Travis        | No Amendments    |
| 1.1     | 03.03.2022 | Project Oversight | Ch. Insp Scott Lloyd   | Minor Amendments |
| 1.2     | 01.05.2023 | Project Oversight | Ch. Insp Scott Lloyd   | Amendments       |



## Contents

|    |                                                                                        |    |
|----|----------------------------------------------------------------------------------------|----|
| 1  | Introduction .....                                                                     | 3  |
| 2  | Application .....                                                                      | 3  |
| 3  | Terminology .....                                                                      | 3  |
| 4  | Authority to Deploy LFR .....                                                          | 3  |
| 5  | ‘Where’ - Date, Time, Duration and Location of Deployment.....                         | 6  |
| 6  | ‘Who’ - Watchlist Generation and Criteria for an Image’s Inclusion on a Watchlist..... | 8  |
| 7  | SWP LFR Documents .....                                                                | 15 |
| 8  | Management of Risk & Resource Levels .....                                             | 16 |
| 9  | Planning & Booking .....                                                               | 17 |
| 10 | LFR Operational Roles .....                                                            | 17 |
| 11 | Post-Deployment .....                                                                  | 20 |
| 12 | LFR Deployment Summary Flowchart .....                                                 | 21 |
| 13 | LFR Application Security.....                                                          | 23 |
| 14 | Data Retention & Data Management .....                                                 | 23 |
| 15 | Contact Information .....                                                              | 24 |
| 16 | Further Documentation.....                                                             | 25 |

|                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Terms &amp; Definitions: Capitalised terms used in this LFR SOP shall have the meaning given to them in the SWP LFR Policy Document unless otherwise defined in this LFR SOP.</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 1 Introduction

- 1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool.

## 2 Application

- 2.1 All South Wales (SWP) police officers and police staff, including the extended police family and those working voluntarily or under contract to the Commissioner must be aware of, and are required to comply with, all relevant SWP policy and associated procedures.
- 2.2 This SOP applies in particular to officers and staff in the following roles:-
  - a) All operational officers and police staff, both uniform or detective, and their supervisors involved in the planning and Deployment of LFR technology; and
  - b) All police officers and police staff involved in any subsequent investigation resulting from the operational Deployment of LFR technology; and
  - c) All Authorising Officers (AO); and
  - d) The operational command team for any LFR Deployment (Gold, Silver and Bronzes); and
  - e) LFR Operators, LFR Engagement Officer and LFR System Engineers.

Note: This list is not intended to be exhaustive.

## 3 Terminology

- 3.1 This SOP focuses exclusively on LFR. Terminology relating to LFR is defined in the SWP LFR Policy Document.

## 4 Authority to Deploy LFR

- 4.1 In normal circumstances the authority given by an AO to deploy LFR in support of a policing operation should be made by an officer not below the rank of Superintendent. Their authorisation should be recorded in writing.
- 4.2 The SWP LFR Application / Written Authority Document recognises that the intelligence case for the use of LFR may give rise to a single Deployment, or a need for a series of Deployments within a time-limited period. Where the SWP LFR Application / Written Authority Document is to be used to authorise a period of up to 7 days during which Deployments may occur, the form provides for a baseline of safeguards to ensure that the need for the Deployment and the currency is the Watchlist continues to be maintained with due oversight. Should the need to Deploy continue beyond 7 days, a further SWP LFR Application / Written Authority Document will be sought. This approach ensures that the use of LFR is time limited but allows an operationally effective way to plan for and deliver LFR as part of wider SWP crime-fighting strategies.

- 4.3 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an SWP officer of NPCC rank<sup>1</sup> must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-South Wales issues are taken into account as much as possible. This affords NPCC the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.
- 4.4 The AO must notify the SWP Police and Crime Commissioner (or designated staff member) prior to any deployment.
- 4.5 Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable.
- 4.6 The authority of the AO:-
- a) must articulate the legitimate aim of the Deployment and the legal powers that are being relied upon to support the Deployment; and
  - b) means that the AO is satisfied that the Deployment complies with SWP LFR documents, or is otherwise authorised; and
  - c) must, from a Human Rights Act 1998 perspective, articulate (i) how and why the Deployment is necessary (and not just desirable), and (ii) is proportionate to achieve the legitimate aim of the Deployment; and
  - d) must, from a Data Protection Act 2018 perspective, articulate that it is strictly necessary for the SWP's law enforcement purposes; meaning there is a 'pressing social need' and it is not reasonably viable to address this through less intrusive means, either because less intrusive tactics have been tried, or it is reasonably believed that those tactics are unlikely to be effective; and
    - i. Necessary on at least one of the following grounds (the ground(s) to be confirmed by AO):-
      - a. Necessary for SWP's lawful policing purposes<sup>2</sup> for reasons of substantial public interest; and / or
      - b. Necessary for the administration of justice; and / or
      - c. Necessary for the safeguarding of children and/or of individuals at risk; and
    - ii. Necessary notwithstanding any expectations people may have pursuant to their Article 8 human rights regarding the respect of private and family life, as well as other human rights considered by the AO; and
  - e) must articulate that the AO has given regard to the safeguards proposed for the Deployment and the safeguards contained within the SWP LFR Documents, and considers that the Deployment in question is a proportionate use of policing powers when considering their use, and balancing them in the context of considerations relating to the Human Rights Act 1998 and the Data Protection Act 2018 and UK GDPR; and

---

<sup>1</sup> NPCC – 'NPCC rank' denotes an officer holding the rank of ACC or above.

<sup>2</sup> This being defined as "is necessary for the exercise of a function conferred on a person by an enactment or rule of law" in the Data Protection Act 2018. This will typically be the ground relied on to support SWP Deployments of LFR since this recognises the policing powers conferred on a Constable.

f) means that the AO is satisfied that all reasonable steps have been taken to ensure that the composition of the Watchlist complies with SWP LFR

Documents, including the legality, necessity and proportionality criteria; and

g) must articulate any authority to include additional categories of persons to the Watchlist, including the legality, necessity and proportionality criteria, in addition to those included to meet the purpose of the Deployment; and

h) means that the AO is directing that all police officers / staff engaged in the Deployment must have received SWP LFR training as per the SWP LFR Documents; and

i) means that the AO considers that the Deployment is proportionate with the benefits anticipated from the use of LFR outweighing the concerns and

impacts there may be in relation to people's human rights and rights relating to equalities; and

j) means that the AO is satisfied that the control measures in the Data Protection Impact Assessment, Community Impact Assessment, and Equality Impact Assessment have been reviewed and considers them to be appropriate mitigants for the Deployment.

k) means the AO has determined the minimum Threshold setting to be utilised during the Deployment. Ordinarily this setting will be equal to or above the value where no FRT System bias is detected (0.64 with the current FRT algorithm). The Threshold value may be lowered based on the intelligence case with a full rationale detailed in the SWP LFR Application / Written Authority Document.

4.7 In cases of urgency an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency. All authorisations must comply with the requirements set out in paragraph 4.6.

4.8 Situations where the need for an authorisation to be granted urgently would

include:-

a) an imminent threat-to-life or of serious harm to people or property; and / or

b) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which supports the urgency of action.

4.9 If an authorisation is given under the urgency criteria above, it shall be the duty of the AO who gives it, to inform an officer of the rank of Superintendent or above as soon as practicable, that LFR has been deployed and the reasons why. It is for the Superintendent to then authorise the Deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

4.10 Should a further law enforcement purpose be identified after the AO has issued their authority for an LFR Deployment, processing in respect of the law enforcement purpose is not permissible unless the AO grants a further authority for it. Such authority would consider the lawfulness, strict necessity and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.

## 5 'Where' - Date, Time, Duration and Location of Deployment

- 5.1 The AO should define the date, time, location and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment.

### Considerations relevant to a LFR Deployment location

The intelligence case, policing purpose to include a person on a Watchlist, Community Impact Assessment and the environmental factors relevant to a potential Deployment location will substantially inform the potential locations for LFR Deployments.

- 5.2 Deployment locations will be determined by there being reasonable grounds to suspect that the proposed Deployment location is one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any selected Deployment location should be recorded and be capable of being considered and evaluated by an objective third person.
- 5.3 The selection of a particular Deployment location may further be supported by:
- a) policing information or intelligence about a proposed Deployment location including if there is an increased public safety risk and/or need to provide public reassurance at a Deployment location; *and*
  - b) the ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so.
- 5.4 When reviewing a potential Deployment location, AOs must also consider those who are likely to pass the LFR System and:
- a) **the reasonable expectations of privacy the general public may have as a whole at that location:**
    - i. some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy Zone 1 central London thoroughfare being typically different to a quiet suburban park or backstreet; and
    - ii. the number of cameras used by the LFR System should also be considered in this context to ensure the size and scale of the Deployment enables those on a Watchlist to be effectively located without disproportionately processing biometric data; *and*
  - b) **if a proposed Deployment location attracts particular concerns by reference to those expected to be at a particular location<sup>3</sup>:**
    - i. hospitals, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), care homes and persons who may be attending a nearby assembly or demonstration are

---

<sup>3</sup> Should a deployment be necessary at a site that is focused on children (for example outside a school), signage and information about the LFR Deployment should typically be reasonably accessible to children who may pass through the Zone of Recognition. Consideration is needed as to the nature of the Deployment and data processing that is proposed and the effectiveness of the mitigations when assessing if a Deployment can be considered proportionate or not.

examples where those that attend them may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area.

- 5.5 Where it is practicable to identify a person of being responsible for a proposed Deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate.
- 5.6 Where privacy or other human rights considerations are identified in relation to a particular Deployment, the AO needs to consider the necessity to Deploy LFR to that particular location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is *necessary* (with the processing of data at that site being *strictly necessary*), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR System against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.

### **Measures during an LFR Deployment**

- 5.7 Save in exceptional operational cases where doing so would undermine objectives or operational imperative of the Deployment (for example, in cases of urgency or where it would compromise other policing tactics) the public should be notified of LFR Deployments in advance using force websites and other appropriate communication channels (including social media).
- 5.8 Measures should also be taken during the Deployment to ensure the policing presence is overt such that the public can establish that LFR is being used and understand the nature of the data being processed. In addition to the use of uniformed officers and marked vehicle(s), other steps for applicants to consider in the context of their proposed Deployment location include the use of signage placed in advance (outside) of the Zone of Recognition and/or the provision of information leaflets. In considering the level of awareness raising measures, whilst a baseline needs to be maintained to ensure that any Deployment is overt, the objectives for the Deployment and its use as a policing tactic will also be relevant if the policing need to deploy is to be realised. For example, unduly extensive signage may undermine the effectiveness of a Deployment seeking to locate persistently outstanding offences. By comparison a Deployment seeking to protect a site or particular event may merit multiple levels of signs and the proactive distribution of leaflets to deter those with mal-intent.
- 5.9 If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of a policing power. SWP staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.
- 5.10 Any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. Any person who requires further information relating to LFR should be provided with contact information for the SWP LFR operational team (FRT@South-Wales.police.uk).

## 6 'Who' - Watchlist Generation and Criteria for an Image's Inclusion on a Watchlist

6.1 This section covers the composition, generation and management of Watchlists to be used in LFR Deployments and is structured to address:

- c) Safeguards relevant to all Watchlists – including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics;
- d) Who may be added to a Watchlist – including in relation to police-originated, and non-police originated imagery;

### Safeguards relevant to all Watchlists

6.2 The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria stipulated in this SWP LFR SOP and be specific to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:-

| Requirement                                                                                                                                                                                                                                                                                                                                                                                                                       | Rationale for the requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Intelligence:</b> Watchlists must be driven by a policing need and based on the intelligence case<br><br>The intelligence case must be current and reviewed before each Deployment.                                                                                                                                                                                                                                            | This intelligence-driven approach ensures that the make-up of the Watchlist is reflective of, and for the purpose of the LFR Deployment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Images sources:</b> Watchlists must only contain images lawfully held by police with consideration also being given as to: <ul style="list-style-type: none"><li>the legal basis under which the image has been acquired; and</li><li>the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.</li></ul> | <p>This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance.</p> <p>Additionally policing has a responsibility to avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.</p> |
| <b>Image selection:</b> Watchlists must only use images where all reasonable steps have been taken to ensure that the image:                                                                                                                                                                                                                                                                                                      | This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that person should they pass the LFR System.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Rationale for the requirement                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>is of a person intended for inclusion on a given Watchlist; and;</li> <li>is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist.</li> </ul> <p>Regard must be paid to the prospect of the LFR System generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken.</p> <p>Regard must also be paid to the ability of the LFR System to operate within the 1:1000 False Alert Rate using the propose image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);</p> | <p>This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The SWP SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.</p> |
| <p><b>Watchlist currency:</b> Watchlists must not be imported into the LFR System more than 24 hours prior to the start of the Deployment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours</p>                                                                                                                                                                                                           |
| <p><b>Watchlist design:</b> Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated</p>                                                                                                                                                    |

### Additional safeguards relating to protected characteristics

- 6.3 Following on from the Bridges case, in December 2020 the then Surveillance Camera Commissioner (SCC) published his best practice guidance document '[Facing the Camera](#)'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist. Any controls, mitigations and processes identified by SWP in this document reflect the SWP LFR System's performance and SWP's particular use-cases for LFR.
- 6.4 SWP has confidence in the LFR System's performance, particularly in relation to gender, age and race.
- 6.5 SWP recognises that *regardless* of performance considerations, it should take particular care when considering and publishing details relating to (i) age including the protection of children



– particularly the very young, (ii) the disabled and (iii) those who have and/or are undertaking a gender reassignment. This is because:

- a) There may be different privacy expectations around the use of LFR<sup>4</sup> and that these can be particularly relevant in relation to these people given their potential vulnerability<sup>5</sup>.
- a) SWP recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.

6.6 Documenting composition: SWP provides that each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be:

- b) aged under 18-years-old;
- c) aged under 13-years-old;
- d) a person with a relevant disability<sup>6</sup>;
- e) a person who has undertaken a gender reassignment and it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment.

6.7 Safeguards regarding composition: The following outlines further, specific safeguards that apply to the composition of the Watchlist:

---

<sup>4</sup> For example, in relation gender reassignment, see Section 22 of the Gender Recognition Act 2004 which protects disclosures other than in certain specific circumstances which include where the disclosure is necessary for the purposes of preventing or investigating crime.

<sup>5</sup> For example, in relation to children, see: <https://www.app.college.police.uk/app-content/detention-and-custody-2/detainee-care/children-and-young-persons/#children-and-young-persons> which is in the context of detention and custody but notes children and young people are a protected group with specific vulnerabilities. Their treatment in detention is governed not only by domestic legislation but also by the [UN Convention on the Rights of the Child \(UNCRC\)](#);

<sup>6</sup> A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) and that such a disability may impact on the performance of the police force's LFR system. Examples which may have an impact (depending on the performance characteristics of the specific LFR system) include if the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised.

|                  | Age (U. 18)                                                                                                                                                                                                  | Age (U.13)                                                                                                                                                                                                                                                                                                                                                                      | Disability                                                                                                                           | Gender Reassignment                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Circumstances    |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
|                  | LFR is used to locate a person under 18 and that person’s records state that person is aged (or suspected to be aged) under 18-years-old                                                                     | LFR is used to locate a person under 18 and that person’s records state that person is aged (or suspected to be aged) under 13-years-old. <sup>7</sup>                                                                                                                                                                                                                          | LFR is to be used to locate a person and that person’s records state that person has (or is suspected to have) a relevant disability | LFR is to be used to locate a person and that person’s records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment |
| Safeguards       |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| Necessity        | Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with SWP LFR Documents with a particular focus on ensuring the necessity case is fully made out. |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| Watchlist Images |                                                                                                                                                                                                              | There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.                                                                                                                                                                                                                                          |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| Legal Advice     |                                                                                                                                                                                                              | Specific advice must be sought from Legal Services and the SWP LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply. |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| Technical Advice | Regard should also be had to consider System and Subject Factors and the ability for the LFR System to generate an accurate Alert against the image proposed for inclusion on the Watchlist.                 |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
|                  | Consideration should be given to the likely crowd flow / occlusion risk where shorter subjects may otherwise be blocked from the camera’s line of sight.                                                     | Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.                                   |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |

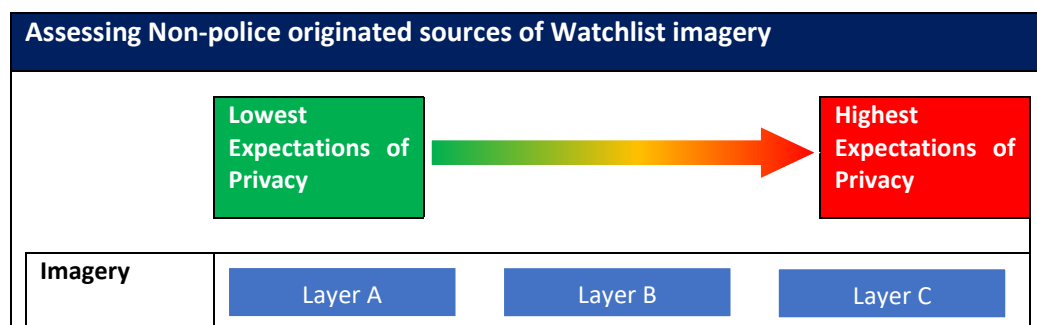
<sup>7</sup> Generally, studies [<https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf>] have shown that young children, up to the age of 13 are both harder to correctly recognise (lower True Positive Identification Rate) but also harder to distinguish between (higher FPIR). The higher FPIR may lead to more False Alerts being generated against young children if there is an image of a young person in the Watchlist.

### Police-originated images that may be included on a Watchlist

- 6.8 Images that may be deemed appropriate for inclusion within an LFR Watchlist include custody images of individuals and/or police originated images other than custody images of people 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 there are reasonable grounds to suspect an individual depicted to be committing an offence; *and/or*
  - c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or*
  - d) missing persons deemed increased risk; *and/or*
  - e) presenting a risk of harm to themselves or others; *and/or*
  - f) who are a 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) – (f).
- 6.9 Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a policing objective and the proportionality of using such images on an LFR System.

### Non-police originated sources of Watchlist imagery

- 6.10 Where it is viable to do so without unduly impacting on the performance of the LFR System, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by SWP or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.
- 6.11 Non-police originated images are images which have not been taken by law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness'.



| Image Layer                                  | Outline                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Non-police originated image – <b>Layer A</b> | <p>Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including:</p> <ul style="list-style-type: none"> <li>• circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage;</li> <li>• circumstances where the police have obtained the image as a result of a lawful power of search or seizure;</li> <li>• data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.</li> </ul>                      |
| Non-police originated image – <b>Layer B</b> | <p>Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject, including any imagery obtained pursuant to:</p> <ul style="list-style-type: none"> <li>• the Regulation of Investigatory Powers Act 2000; and</li> <li>• the Investigatory Powers Act 2016,</li> </ul> <p>where the ability of relevant bodies to obtain such images is further supported and can be anticipated by reference to published Codes of Practice.</p>                                                                                                                                                                                                                                                                                                                 |
| Non-police originated image – <b>Layer C</b> | <p>Non-police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received.</p> <p>To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.</p> |

6.12 Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular which layer of intrusiveness the image is attributable to and the factors at paragraph 6.11 above.

6.13 The types of non-police originated images that may be deemed appropriate for inclusion within an LFR Watchlist are of people:

- 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 there are reasonable grounds to suspect an individual depicted to be committing an offence; *and/or*
- c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or* (d) missing persons deemed increased risk; *and/or*
- e) presenting a risk of harm to themselves or others; *and/or*

f) who are a 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) – (f).

- 6.14 **‘Wanted by the courts’**. This term includes those with outstanding arrest warrants or who are otherwise required by the courts. The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general.
- 6.15 **‘Missing persons deemed increased risk.’** This term will be subject to the College of Policing definition of medium risk (or above) that is contained in the Missing Persons APP, meaning that the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public. A decision to include a missing person on the watchlist should take into account the individual circumstances of each case, including the impact it may have on the missing person and their expectations or privacy.
- 6.16 **‘Presenting a risk of harm’**. Mitigating the risk of harm to themselves or to others will need to have a legal basis for action under a policing common law power. ‘Harm’ can include a risk of harm arising in relation to a person’s welfare and/or a financial harm including as a result of fraud or other dishonesty. It can also include ‘Harm’ in the context of posing a risk to national security.
- 6.17 The risk of harm will be informed by the intelligence case and/or the considerations set out in the applicable LFR form. This will need to inform the AO as to how the individual or group of individuals<sup>8</sup> present(s) a risk of harm to themselves or to others and:
- a) how using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*
  - b) why the significance of the harm identified means it is **necessary** for the police to take action in order to manage the risk.
- 6.18 The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:
- a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
  - b) the importance of locating the person or people sought with reference to the threat, harm and risk<sup>9</sup> which the addition to the Watchlist addresses;
  - c) whether the significance of the threat, harm and risk identified, which inclusion on the watchlist would address outweighs any expectations of privacy.
- 6.19 **Victim of an offence, or a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation,**

---

<sup>8</sup> A group of individuals may be added to the watchlist where each individual within the group meets a criterion that would justify addition to the watchlist.

<sup>9</sup> Including for the purposes of taking preventative measures against the occurrence (or future occurrence) of the relevant threat, harm and risk.

**or is otherwise a close associate of an individual.** This criteria includes a victim, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within paragraphs 6.8 (a) – (e) and 6.13 (a) – (e) of the categories that may be deemed appropriate for inclusion within an LFR Watchlist. The threshold for any Watchlist inclusion is high and the use of the category will be by exception; the necessity for inclusion must be based on a specific intelligence-case with the need for the inclusion on a Watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to be able to demonstrate to the AO's satisfaction:

- a) why the inclusion of each victim, person reasonably suspected of having information, or close associate is **necessary** to help locate the person who is wanted by the courts and/or the police; *and/or*
- b) why locating each victim, person reasonably suspected of having information, or close associate person is **necessary** to advance the policing investigation; *and/or*
- c) why locating each victim, person reasonably suspected of having information, or close associate is **necessary** to ensure their safety and/or the safety of others

6.20 The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

- a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
- b) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;
- c) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any inclusion on the Watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others.

## 7 SWP LFR Documents

7.1 Assessments; For each authorised LFR operation, the following assessments need to be created, reviewed, and amended where necessary:-

- (i) Data Protection Impact Assessment\* (Review/Amend/Adopt); and
- (ii) Equality Impact Assessment\* (Review/Amend/Adopt); and
- (iii) Community Impact Assessment\* (Review/Amend/Adopt); and
- (iv) The Surveillance Camera Commissioner's Self-Assessment\* (Review/Amend/Adopt);

Note: \*Any assessment listed above showing 'Review/Amend/Adopt' has already been created by the SWP LFR team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each LFR operation.

## 8 Management of Risk & Resource Levels

- 8.1 Each Deployment should be risk assessed in line with SWP procedure. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.
- 8.2 The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.
- 8.3 Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.
- 8.4 LFR System Engineers will be deployed to support LFR Deployments and will come with suitable vehicles where required.
- 8.5 All SWP officers and staff deployed on LFR Deployments must be compliant and in date with SWP First Aid and where applicable officer safety (OST) training requirements. All SWP officers and staff involved in an LFR Deployment must receive LFR training prior to being deployment.

## 9 Planning & Booking

- 9.1 As part of the LFR planning process and before the AO authorises a Deployment, the SWP LFR team (including LFR System Engineers) should be consulted on the appropriateness and viability of a Deployment.

## 10 LFR Operational Roles

### **LFR Command Team**

- 10.1 LFR Deployments must be supported with a clear command structure. The following roles are defined for the purpose of creating an appropriate hierarchical command structure:-

a) Gold Commander (Superintendent or above<sup>10</sup>); There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their 'strategic intention' aligns with the Written Authority Document. Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold will also liaise as necessary with NPCC ranked officers. Gold can also perform the AO role.

b) Silver Commander (Chief Inspector or above); There is only one Silver Commander for any LFR Deployment. Silver reports to Gold. Silver has tactical command of the Deployment and is responsible for tactical implementation. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having particular regard to the effectiveness of the safeguards in place whilst LFR is being used.

c) Bronze Commander (Sergeant or above); Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze

Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with sufficient clarity, and ensure that they are fully understood by all officers and staff involved in the Deployment.

- 10.2 Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative command team terminology, or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

### **LFR Operator**

- 10.3 LFR Operators receive detailed training prior to being deployed operationally. Their role is to monitor and assess application Alerts, before working with LFR Engagement Officers (as necessary) to decide whether an Engagement is required.

---

<sup>10</sup> Note that where the urgency criteria (para 4.4) has been applied, the Gold Commander may be of Inspecting rank. However, this should revert to Superintendent or above as soon as a

Superintendent reviews the Deployment and provides authority for the Deployment to continue.



- 10.4 The LFR Operator must log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR System performance to the Silver Commander.
- 10.5 The LFR Operator's log should include:-
- a) the LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; and
  - b) what decision was taken regarding whether to Engage a member of the public or not; and
  - c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

### **LFR Engagement Officer**

- 10.6 LFR Engagement Officers must have an understanding of the LFR application, how it performs, and what effect Subject, System, and Environmental Factors might have.
- These officers must receive a full operational briefing prior to deployment. These officers may be deployed in uniform or plain clothes.
- 10.7 When conducting an Engagement, LFR Engagement Officers must ensure that they do so lawfully, and in an appropriate and proportionate manner. Officers must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject of an Engagement, should be supplied with an LFR information leaflet.
- 10.8 The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place<sup>11</sup>. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.
- 10.9 When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal.
- 10.10 Whilst officers must exercise their own discretion when using their powers of arrest and detention, SWP policy is that an LFR application-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.

---

<sup>11</sup> The driving force behind this point is that an LFR Operator should not be making the decision that an Engagement Officer carries out an Engagement. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own 'reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take.

- 10.11 If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.
- 10.12 After any Engagement (that follows an Alert), the LFR Engagement Officer must update the LFR Operator with the outcome of that Engagement.
- 10.13 Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, 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.

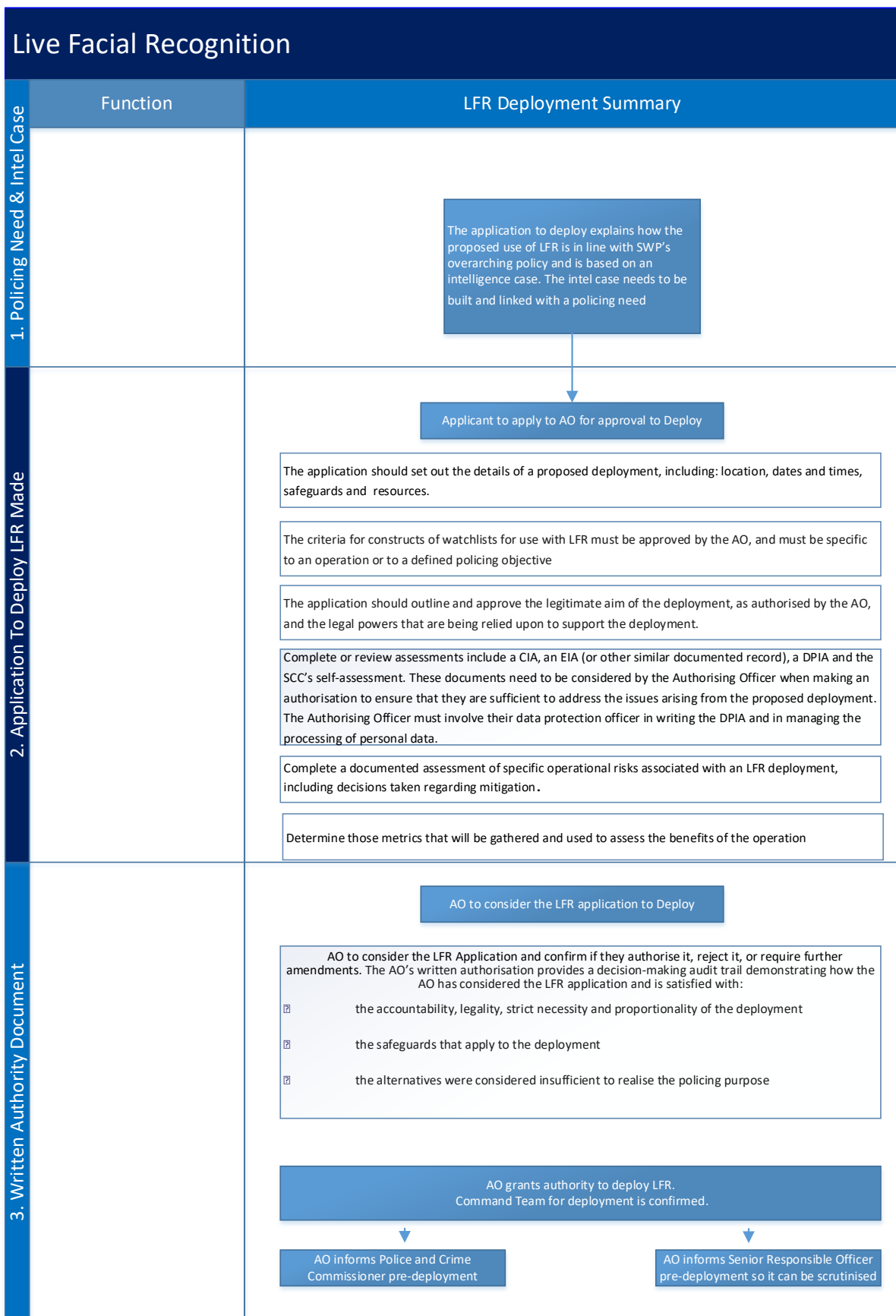
#### **LFR System Engineers**

- 10.14 LFR System Engineers have enhanced technical training for the Deployment of LFR (see SWP LFR Policy Document for further information). LFR System Engineers are responsible for the set-up of the LFR equipment and the optimisation of the LFR application to maximise performance.

## 11 Post-Deployment

- 11.1 Following each LFR Deployment, the Silver Commander must ensure that a post Deployment evaluation is completed which is updated in the Deployment Record. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both qualitative and quantitative in nature.
- 11.2 The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the Deployment and what opportunities exist to improve them for future use, and how learning will be shared.
- 11.3 The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (including what methods were used to obtain them):-
  - a) total number of individuals and the total number of images included in the Watchlist (there may be multiple images of some individuals); and
  - b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR application was able to generate a Template from them); and
  - c) total number of LFR application-generated Alerts; and
  - d) total number of Alerts that do not result in an Engagement; and
  - e) total number of Alerts where a decision was taken to Engage an individual; and
  - f) total number of Alerts that are confirmed as true alert (the individual is who the LFR application suggests are); and
  - g) total number of Alerts that are confirmed as a false alert (the individual is not who the LFR application suggests they are); and
  - h) total number of correct Alerts that result in an Engagement that do not require any further police action; and
  - i) outcome of each case where police action is instigated following an Alert; and
  - j) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome; and
  - k) Threshold setting for the Deployment

# 12 LFR Deployment Summary Flowchart

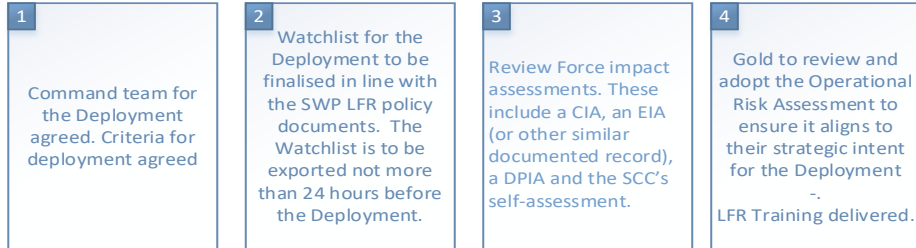


# Live Facial Recognition

Pre-Deployment Activity

## LFR Deployment Summary

Completion of LFR application explaining how the proposed use of LFR is based on an intelligence case. The AO considers the application and records decision in a written authority document. Performance metrics determined



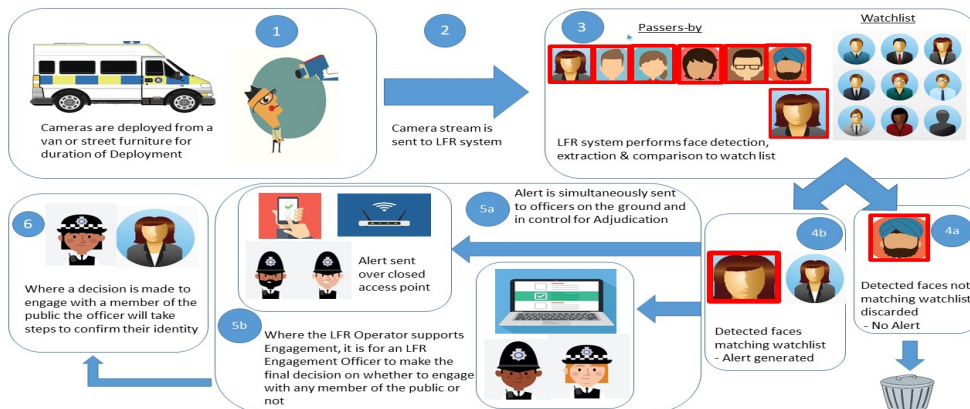
LFR Deployment

Public engagement measures implemented to support the overt use of LFR to locate persons on a Watchlist and to support data subjects being aware of their individual rights.

Watchlist should be imported into the LFR application immediately prior to deployment and no more than 24 hours prior to the commencement – where the deployment is to last in excess of 24 hours, there must be an ongoing review, covering the issues of review, retention and deletion

LFR Deployment undertaken. The Deployment is to remain under review in line with the AO's authority and the assessments which support the Deployment. Key metrics are to be recorded to support the ongoing assessment of LFR performance and to aid transparency with the public post-Deployment.

Summary of typical LFR deployment.



Post-Deployment Activity

Cancellation report including

- where and when of the deployment
- the circumstances that ended deployment
- what resources were used
- relevant statistics
- outcomes

a summary of any issues following a post-deployment review

Data only to be retained where it is necessary to do so and it should be retained and managed in line with SWP LFR DPIA / SWP LFR Policy

Register of Deployments to be updated and published.

## 13 LFR Application Security

- 13.1 The LFR application includes a number of physical and technical security measures. These include:-
- a) images are transferred onto the LFR application via an encrypted USB device or via a secure Connection to the SWP Virtual Private Network ; and
  - b) the LFR application is a fully-closed system with two layers of password protection to access the application; and
  - c) the LFR application is physically protected when in use and deployment data stored on the system is securely wiped following each Deployment; and
  - d) role based access controls with limited user permissions are implemented on the LFR application; and
  - e) the LFR application can be connected to mobile devices using a private access point with three levels of protection; Specific IP addressing, password access to the access point, and password access to the mobile App. The mobile App has a RESTful API and will be covered by SSL; and
  - f) the Dashboard and RESTful API are secured with SSL and TLS by default; and all connections are directed through HTTPS; and
  - g) a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; and
  - h) technical issues with the LFR application are always dealt with by LFR System Engineers deployed on the operation.

## 14 Data Retention & Data Management

- 14.1 The SWP must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the SWP LFR Documents. This means that:-
- a) where the LFR application does not generate an Alert, that a person's biometric data is immediately automatically deleted; and
  - b) the data held on the encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours, following the conclusion of the Deployment.
- 14.2 Where the LFR application generates an Alert, all personal data is deleted as soon as practicable and in any case within 24 hours.
- 14.3 All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-
- a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; and /or
  - b) in accordance with the SWP's complaints / conduct investigation policies.

c) To support compliance the LFR application has a full audit capability, and the LFR Operator and LFR Engagement Officer log is retained in line with MOPI retention periods.

d) The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether or not protected by encryption, must be reported immediately to the AO, Gold, and the SWP Data Protection Officer.

### **Register of Deployments**

Any Deployment of LFR must be recorded on a centrally held register. This register will record a number of things including:-

- a) name and rank of the AO and command team; and
- b) date, time, duration, and locality of Deployment; and
- c) Watchlist composition statistics (not including any personal data); and
- d) the number of Alerts and the various statistics relating to these; and
- e) number of Engagements and their results;

- 14.7 The SWP will make information relating to LFR Deployments available to the public in accordance with the SWP LFR Documents.

## **15 Contact Information**

- 15.1 The SWP LFR team can be contacted using the following email address; [FRT@South-wales.police.uk](mailto:FRT@South-wales.police.uk).

## 16 Further Documentation

16.1 Further documentation is available providing useful information relevant to LFR. This is detailed below.

- a) Information Management APP;  
[www.app.college.police.uk/appcontent/information-management](http://www.app.college.police.uk/appcontent/information-management);
- b) National Decision Model; [www.app.college.police.uk/app-content/nationaldecision-model](http://www.app.college.police.uk/app-content/nationaldecision-model);
- c) National Intelligence Management;  
[www.app.college.police.uk/appcontent/intelligence-management](http://www.app.college.police.uk/appcontent/intelligence-management);
- d) College of Policing Code of Ethics; [www.app.college.police.uk/code-ofethics](http://www.app.college.police.uk/code-ofethics);
- e) Home Office Biometric Strategy – Published June 2018;  
[www.gov.uk/government/publications/home-office-biometrics-strategy](http://www.gov.uk/government/publications/home-office-biometrics-strategy);
- f) High Court Ruling – R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341 (Admin);  
[www.judiciary.uk/wpcontent/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf](http://www.judiciary.uk/wpcontent/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf).





|                         |                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protective marking:     | Official                                                                                                                                               |
| Publication scheme Y/N: | No                                                                                                                                                     |
| Title:                  | Standard Operating Procedure for the Overt Operational Deployment of Live Facial Recognition (LFR) Technology                                          |
| Version:                | Version 2.0                                                                                                                                            |
| Summary:                | Establishes procedures for the Deployment of Live Facial Recognition (LFR) technology in support of policing operations to locate those on Watchlists. |
| Branch/ OCU:            | MPS LFR                                                                                                                                                |
| Review date:            | 29 <sup>th</sup> November 2022                                                                                                                         |

## **STANDARD OPERATING PROCEDURE (SOP) FOR THE OVERT DEPLOYMENT OF LIVE FACIAL RECOGNITION (LFR) TECHNOLOGY**

**Terms & Definitions:** Capitalised terms used in this LFR SOP shall have the meaning given to them in the MPS LFR Policy Document unless otherwise defined in this LFR SOP.

### **1 Introduction**

- 1.1 This Standard Operating Procedure (SOP) explains the standard procedures to be adopted when planning for and using Live Facial Recognition (LFR) technology in an overt way to locate those on Watchlists and in support of policing operations. Compliance with the SOP will help ensure a corporate response to the use of this policing tool. As part of a published suite of documents, this also allows the public passing an LFR system and those who may be placed on a Watchlist to understand the standards the Metropolitan Police Service (MPS), as a public body, operates to. In doing so, the MPS provides details about the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

To help set the standard operating procedures in context, a summary flowchart has been produced and is annexed to this SOP. It shows the various stages required to plan for and deliver an LFR Deployment.

## 2 Application

- 2.1 All MPS police officers and police staff and those who support the extended police family (including those working voluntarily or under contract) must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.
- 2.2 This SOP applies in particular to officers and staff in the following roles:-
- a) All operational officers (both uniform or detective) and police staff and their supervisors involved in the planning and Deployment of LFR technology; *and*
  - b) All police officers and police staff involved in any subsequent investigation resulting from the operational Deployment of LFR technology; *and*
  - c) All Authorising Officers (AO); *and*
  - d) The operational command team for any LFR Deployment (Gold, Silver and Bronzes); *and*
  - e) LFR Operators and LFR System Engineers.

**Note:** This list is not intended to be exhaustive.

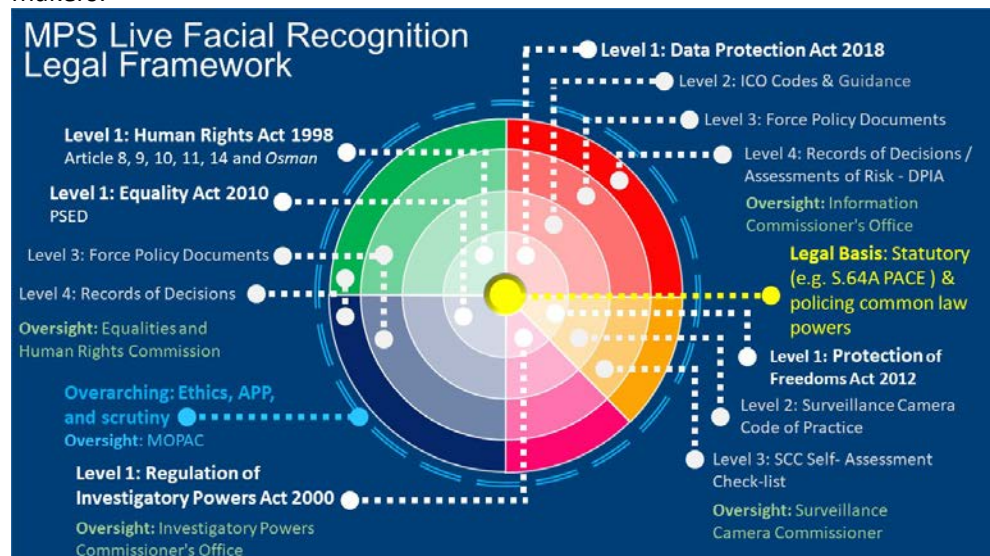
## 3 Terminology

- 3.1 This SOP focuses exclusively on LFR. Terminology relating to LFR is defined in the MPS LFR Policy Document.

## 4 Authority to Deploy LFR

### The legal framework to Deploy LFR

- 4.1 The legal framework, which underpins the application and authority process to deploy LFR, is set out in the MPS LFR Mandate. How that framework comes together is also summarised in the schematic below in order to assist applicants and decision makers:



- 4.2 The legal framework schematic is best read from the inside of the diagram out in the following way:

| Legal Framework Schematic Key: |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Yellow centre</b>           | This is the legal basis for the action – i.e. the legal power(s) that supports the compilation of the Watchlist and the use of LFR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Red segment</b>             | This area reflects that biometric and other personal data is processed by the LFR system. It reflects the application of the Data Protection Act 2018 and underlying documents that govern and reflect this.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Green segment</b>           | This area reflects the relevance of human rights to the use of LFR. Some, like the right to privacy, will be engaged by those on the LFR Watchlist and/or passing the LFR system. The engagement of other rights will be context dependant.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Blue Segment</b>            | This area reflects the relevance of equality considerations and the application of the Public Sector Equality Duty. It shows the underlying documents which also govern and show compliance with this duty.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Pink Segment</b>            | This area reflects the potential application of the Regulation of Investigatory Powers Act 2000 (RIPA). For an overt capability, it is important to have regard to RIPA to ensure the use of LFR does not become directed surveillance.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Orange Segment</b>          | This area reflects that LFR uses CCTV cameras to film those passing through the Zone of Recognition as part of the wider LFR system. It recognises the relevance of the Protection of Freedoms Act 2012 to CCTV in public spaces by policing in England and Wales.                                                                                                                                                                                                                                                                                                                                   |
| <b>Level 1</b>                 | <b>Primary legislation:</b> This level of the legal framework reflects a statutory legislation enacted by Parliament that combines in its application to provide a framework for the regulation of LFR.                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Level 2</b>                 | <b>Secondary legislative instruments:</b> This level of the legal framework reflects statutory codes and non-statutory guidance typically issued at a national level which Chief Officers should have regard to when seeking to apply the Level 1 legal framework.<br>Authorised Professional Practice (APP) issued by the College of Policing also sits at this level within the legal framework. However, given some APP is not specific to a particular area of primary legislation, it is reflected as an overarching consideration in the legal schematic to reflect its pervasive application. |
| <b>Level 3</b>                 | <b>Force policy:</b> This reflects policy documents issues at a force level. They provide for the operational implementation of the legal framework in a way that helps the use of LFR to be both accessible and foreseeable to the public.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Level 4</b>                 | This level of documentation reflects the use of the legal framework in practice – ensuring relevant decisions, including the rationale, necessity and proportionality for use is recorded. It is also the place where decisions of relevance to the Public Sector Equality Duty should be recorded.                                                                                                                                                                                                                                                                                                  |
| <b>Overarching:</b>            | The all-encompassing <a href="#">blue dashed line</a> shows that there are a number of aspects to the lawful and ethical use of LFR systems which are pervasive and do not just relate to one area of law.                                                                                                                                                                                                                                                                                                                                                                                           |

### **Applying to Deploy LFR**

- 4.3 An applicant may seek the authorisation to deploy LFR via the MPS LFR Form 1, Part 1 – Application. The MPS LFR Form 1 is annexed to this SOP to assist readers with the requirements to apply for and authorise an LFR Deployment.
- 4.4 In normal circumstances the authorisation given by an AO to Deploy LFR in support of a policing operation should be made by an officer not below the rank of Superintendent. Their authorisation should be recorded in writing via the MPS LFR Form 1, Part 2 – Written Authority Document.
- 4.5 Prior to AO authorisation and the Deployment of LFR in public spaces, a number of documents must be completed and an MPS officer of NPCC rank<sup>1</sup> must be engaged by the AO. Whilst NPCC do not provide authority for LFR Deployment, consultation at this level exists so as to expose the proposed Deployment to an elevated level of strategic thinking, whereby pan-London issues are taken into account as much as possible. This affords NPCC the opportunity to veto the Deployment altogether, or to ask the AO to consider what mitigation is required to address concerns at hand.
- 4.6 Where an AO is not immediately able to provide their decision in writing, their authorisation may be given verbally. Verbal authorisation must then be recorded in writing by the AO as soon as is practicable via the MPS LFR Form 1, Part 2 – Written Authority Document.
- 4.7 Should a further law enforcement purpose be identified after the AO has issued their authorisation for an LFR Deployment, processing in respect of the law enforcement purpose is not permissible unless the AO grants a further authority for it. Such authority would consider the lawfulness, strict necessity and proportionality of using LFR to meet the law enforcement purpose and its compatibility with the original law enforcement purpose.
- 4.8 Urgency: In cases of urgency an officer below the rank of Superintendent, but not below the rank of Inspector, may authorise the Deployment of LFR in support of a police operation if they are satisfied that such authorisation is required as a matter of urgency. All authorisations must comply with the requirements set out in paragraph 4.3.
- 4.9 Situations where the need for an authorisation to be granted urgently would include:-
- a) an imminent threat-to-life or of serious harm to people or property; *and / or*
  - b) an intelligence / investigative opportunity with limited time to act, the seriousness and benefit of which supports the urgency of action.
- 4.10 If an authorisation is given under the urgency criteria above, it shall be the duty of the AO who gives it, to inform an officer of the rank of Superintendent or above as soon as practicable, that LFR has been deployed and the reasons why. It is for the

---

<sup>1</sup> NPCC – ‘NPCC rank’ denotes an officer holding the rank of Commander or above.

Superintendent (or higher-ranking) to then authorise the Deployment to continue, making changes to the authority as they deem necessary, or direct that it must stop.

## 5 ‘Where’ - Date, Time, Duration and Location of Deployment

- 5.1 The AO should define the date, time, location and duration the Deployment is authorised for based on the principles of necessity and proportionality in pursuing a legitimate policing aim, informed by the intelligence case behind the Deployment.

### **Considerations relevant to a LFR Deployment location**

- 5.2 The intelligence case, policing purpose to include a person on a Watchlist and Community Impact Assessment will substantially inform the potential locations for LFR Deployments.
- 5.3 The Deployment location will be determined by there being reasonable grounds to suspect that the proposed Deployment location is one at which one or more persons on the Watchlist will attend at a time or times at which they are to be sought by means of LFR. The reasons for any selected Deployment location should be recorded and be capable of being considered and evaluated by an objective third person.
- 5.4 The selection of a particular Deployment location may further be supported by:
- a) policing information or intelligence about a proposed Deployment location including if there is an increased public safety risk at a Deployment location; *and*
  - a) the ability for the police to take action as a result of an alert being generated to make engagements with the public where it is lawful, necessary and proportionate to do so.
- 5.5 When reviewing a potential Deployment location, AOs must also consider those who are likely to pass the LFR system and:
- a) **the reasonable expectations of privacy the general public may have as a whole at that location:**
    - i. some places by their nature attract greater privacy expectations than others with, for example, the expectations at a busy Zone 1 central London thoroughfare being typically different to a quiet suburban park or backstreet; and
    - ii. the number of cameras used by the LFR system should also be considered in this context to ensure the size and scale of the Deployment enables those on a Watchlist to be effectively located without disproportionately processing excessive biometric data; *and*
  - b) **if a proposed Deployment location attracts particular concerns by reference to those expected to be at a particular location<sup>2</sup>:**

---

<sup>2</sup> Should a deployment be necessary at a site that is focused on children (for example outside a school), signage and information about the LFR Deployment should typically be reasonably

- i. hospitals, places of worship, centres for legal advice, polling stations, schools (and other places particularly frequented by children), care homes and persons who may be attending a nearby assembly or demonstration are examples where those that attend them may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area.
- 5.6 Where it is practicable to identify a person of being responsible for a proposed deployment location, and that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate.
- 5.7 Where privacy or other human rights considerations are identified in relation to a particular Deployment, the AO needs to consider the necessity to Deploy LFR to that particular location and whether the aims being pursued could be similarly achieved elsewhere. In instances where that location is *necessary* (with the processing of data at that site being *strictly necessary*), AOs then need to identify any mitigations that are viable in the circumstances and then weigh the rights of those engaged by the LFR system against the likely benefits of using LFR. This is to ensure the policing action proposed is not disproportionate to the aim being pursued.

#### **Measures during an LFR Deployment**

- 5.8 During any policing operation where LFR is Deployed in line with SOP, signs publicising the use of the technology should be prominently placed in advance (outside) of the Zone of Recognition. These measures are to alert members of the public of the presence of LFR technology and allow them sufficient time to exercise their right not to walk into the Zone of Recognition.
- 5.9 The public should also be notified of LFR Deployments in advance, save in exceptional cases where doing so would undermine objectives or operational imperative of the Deployment (for example, in cases of urgency or where it would compromise other policing tactics). Details of the LFR Deployment are to be notified to the public using force websites and other appropriate communication channels (including social media).
- 5.10 If a person decides not to walk through the Zone of Recognition this action does not in itself justify the use of a policing power. MPS staff deployed to this operation must be accountable for their own actions and must exercise their powers in accordance with the law and the Code of Ethics.
- 5.11 Any member of the public who is Engaged as part of an LFR Deployment should, in the normal course of events, also be offered an information leaflet about the technology. Any person who requires further information relating to LFR should be provided with contact information for the MPS LFR operational team (LFR@met.police.uk).

---

accessible to children who may pass through the Zone of Recognition. Consideration is needed as to the nature of the Deployment and data processing that is proposed and the effectiveness of the mitigations when assessing if a Deployment can be considered proportionate or not.

## 6 'Who' - Watchlist Generation and Criteria for an Image's Inclusion on a Watchlist

6.1 This section covers the composition, generation and management of Watchlists to be used in LFR Deployments and is structured to address:

- a) Safeguards relevant to all Watchlists – including safeguards which apply to all Watchlists and further safeguards which have been adopted in relation to certain protected characteristics;
- b) Who may be added to a Watchlist – including in relation to police-originated, and non-police originated imagery;
- c) The approach to be taken to Additional Watchlist Categories – this being relevant where the need to undertake a Deployment is already made out by reference to the primary Watchlist and the intelligence case supports the use that the Deployment to locate further persons, for example those wanted by the courts - such additional purpose must also be necessary and proportionate.

### Safeguards relevant to all Watchlists

6.2 The criteria for the construction of the Watchlist for use with LFR must be approved by the AO, fall within the criteria stipulated in this MPS LFR SOP and be specific to an operation or to a defined policing objective. Watchlists, and the images for inclusion on a Watchlist must comply with the following requirements:-

|    | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                           | Rationale for the requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <b>Intelligence:</b> Watchlists must be driven by a policing need and based on the intelligence case<br><br>The intelligence case must be current and reviewed before each Deployment.                                                                                                                                                                                                                                                | This intelligence-driven approach ensures that the make-up of the Watchlist is honed to, and not excessive for the purpose of the LFR Deployment                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 2. | <b>Images sources:</b> Watchlists must only contain images lawfully held by police with consideration also being given as to: <ul style="list-style-type: none"><li>• the legal basis under which the image has been acquired; and</li><li>• the source of the image, particularly where the image is derived from a sensitive or third-party source and may risk compromising that source or exposing that source to risk.</li></ul> | This requirement ensures that all images proposed for inclusion are lawfully held by the police – this includes consideration of the legal basis, human rights (including intrusion) and data protection considerations. This ensures that in all cases, the lawfulness and intrusion caused by using the image is considered and justified. It also ensures that where the legal basis limits how the police hold and process an image (for example for what purposes it may be used), this is considered to ensure legal compliance.<br><br>Additionally policing has a responsibility to |



|    | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Rationale for the requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | avoid compromising policing tactics or exposing sources to risk – this requirement covers this point.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 3. | <p><b>Image selection:</b> Watchlists must only use images where all reasonable steps have been taken to ensure that the image:</p> <ul style="list-style-type: none"> <li>• is of a person intended for inclusion on a given Watchlist; and;</li> <li>• is the most up to date and/or suitable image available to the police that is of appropriate quality for inclusion on the Watchlist.</li> </ul> <p>Regard must be paid to the prospect of the LFR system generating an Alert should an older image be proposed for inclusion where the person's facial features may have changed or aged significantly since the image was taken.</p> <p>Regard must also be paid to the ability of the LFR system to operate within the 1:1000 False Alert Rate using the propose image and if there is a need to adjust a Threshold in relation to the proposed image (at the outset or as part of the ongoing responsibilities of the LFR Operator);</p> | <p>This requirement is to ensure that the act of placing a person on a Watchlist is best aligned with locating that person should they pass the LFR system.</p> <p>This requirement and the prescribed False Alert Rate is also designed to minimise the likelihood of unduly inconveniencing others not of interest to policing whilst ensuring those sought are located. The MPS SRO for LFR has determined the 1:1000 False Alert Rate represents an approach which balances these factors in a proportionate way.</p> |
| 4. | <p><b>Watchlist currency:</b> Watchlists must not be imported into the LFR system more than 24 hours prior to the start of the Deployment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>This is to ensure the ongoing currency of a Watchlist should a Deployment be necessarily undertaken for a period of longer than 24 hours</p>                                                                                                                                                                                                                                                                                                                                                                           |
| 5. | <p><b>Watchlist design:</b> Watchlists should benefit from technical measures being adopted through the segregation within the Watchlist.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>This is to ensure the status of those on a Watchlist is recognised by those involved in undertaking Engagements in order to ensure the appropriate action is taken should an Alert be generated</p>                                                                                                                                                                                                                                                                                                                    |

### Additional safeguards relating to protected characteristics

- 6.3 Following on from the Bridges case, in December 2020 the then Surveillance Camera Commissioner (SCC) published his best practice guidance document 'Facing the Camera'. The SCC advocated the need to ensure suitable controls exist around the placing of persons with protected characteristics on a Watchlist. Any controls,

mitigations and processes identified by the MPS in this document reflect the MPS LFR system's performance and the MPS's particular use-cases for LFR.

- 6.4 The MPS explains how it has confidence in the LFR system's performance, particularly in relation to gender and race in its published document, the Metropolitan Police Service Live Facial Recognition System; Understanding Accuracy and Bias
- 6.5 The MPS also recognises that *regardless* of performance considerations, it should take particular care when considering and publishing details relating to (i) age including the protection of children – particularly the very young, (ii) the disabled and (iii) those who have and/or are undertaking a gender reassignment. This is because:
  - a) There may be different privacy expectations around the use of LFR<sup>3</sup> and that these can be particularly relevant in relation to these people given their potential vulnerability<sup>4</sup>.
  - b) The MPS recognises that those involved in criminality have the wherewithal and capability to exploit information to their advantage. This may arise if there is a published performance differential that shows a lower performance level in relation to a particular protected characteristic.
- 6.6 Documenting composition: The MPS provides that each Deployment must specifically identify and document whether the Watchlist contains persons who are believed or suspected to be:
  - c) aged under 18-years-old;
  - d) aged under 13-years-old;
  - e) a person with a relevant disability<sup>5</sup>;
  - f) a person who has undertaken a gender reassignment and it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment.

---

<sup>3</sup> For example, in relation gender reassignment, see Section 22 of the Gender Recognition Act 2004 which protects disclosures other than in certain specific circumstances which include where the disclosure is necessary for the purposes of preventing or investigating crime.

<sup>4</sup> For example, in relation to children, see: <https://www.app.college.police.uk/app-content/detention-and-custody-2/detainee-care/children-and-young-persons/#children-and-young-persons> which is in the context of detention and custody but notes children and young people are a protected group with specific vulnerabilities. Their treatment in detention is governed not only by domestic legislation but also by the [UN Convention on the Rights of the Child \(UNCRC\)](#);

<sup>5</sup> A relevant disability in this context means those with a disability (as the term is defined in section 6(1) of the Equality Act 2010) and that such a disability may impact on the performance of the police force's LFR system. Examples which may have an impact (depending on the performance characteristics of the specific LFR system) include if the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised.

- 6.7 Safeguards regarding composition: The following outlines further, specific safeguards that apply to the composition of the Watchlist:

|                         | Age (U. 18)                                                                                                                                                                                                      | Age (U.13)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Disability                                                                                                                           | Gender Reassignment                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Circumstances</b>    |                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
|                         | LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 18-years-old                                                                         | LFR is used to locate a person under 18 and that person's records state that person is aged (or suspected to be aged) under 13-years-old <sup>6</sup>                                                                                                                                                                                                                                                                                                                                                                                      | LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) a relevant disability | LFR is to be used to locate a person and that person's records state that person has (or is suspected to have) (i) undertaken a gender reassignment and (ii) it is believed or suspected to be that the Watchlist would be using an image of that person taken prior to their reassignment |
| <b>Safeguards</b>       |                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| <b>Necessity</b>        | Specific regard needs to be had for the importance of locating the subject on a risk-based approach in line with the MPS LFR Documents with a particular focus on ensuring the necessity case is fully made out. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| <b>Watchlist Images</b> |                                                                                                                                                                                                                  | There is a particular need to ensure that the image is a current as possible and of a suitable quality for inclusion on the Watchlist.                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| <b>Legal Advice</b>     |                                                                                                                                                                                                                  | Specific advice must be sought from the Directorate of Legal Services and the MPS LFR team prior to any seeking authorisation from an AO. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply.                                                                                                                                         |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |
| <b>Technical Advice</b> |                                                                                                                                                                                                                  | Regard should also be had to consider System and Subject Factors and the ability for the LFR system to generate an accurate Alert against the image proposed for inclusion on the Watchlist. Technical advice should be sought on a case-by-case basis to inform this assessment. Where authorisation is then sought, this advice needs to be provided to the AO to help inform their decision making and allow the AO to record their decision regarding any inclusion on the Watchlist and outline further safeguards that should apply. |                                                                                                                                      |                                                                                                                                                                                                                                                                                            |

<sup>6</sup> Generally, studies [<https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf>] have shown that young children, up to the age of 13 are both harder to correctly recognise (lower True Positive Identification Rate) but also harder to distinguish between (higher FPIR). The higher FPIR may lead to more False Alerts being generated against young children if there is an image of a young person in the Watchlist.

### **Police-originated images that may be included on a Watchlist**

- 6.8 Images that may be deemed appropriate for inclusion within an LFR Watchlist include custody images of individuals and/or police originated images other than custody images of people 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 there are reasonable grounds to suspect an individual depicted to be committing an offence; *and/or*
  - c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or*
  - d) missing persons deemed increased risk; *and/or*
  - e) presenting a risk of harm to themselves or others; *and/or*
  - f) who are a 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).
- 6.9 Where police originated images other than custody images are considered for use, consideration regarding the inclusion of such images is needed. Such consideration requires a case-by-case assessment. Relevant factors in that assessment may include the purpose for which the police hold such images, any processing limitations attached to the images, the importance of including such images on a Watchlist in order to meet a policing objective and the proportionality of using such images on an LFR system.

### **Non-police originated sources of Watchlist imagery**

- 6.10 Where it is viable to do so without unduly impacting on the performance of the LFR system, suitable police-originated images should be preferred for inclusion on a Watchlist. However, there will be occasions, where no image is held by the MPS or the wider law enforcement community, or if one is held, its quality or currency is not optimal for facial recognition purposes. In these circumstances, consideration may be given to the inclusion of a non-police originated image.
- 6.11 Non-police originated images are images which have not been taken by law enforcement. The expectations of privacy, and the intrusion associated with such images can vary depending on the nature of the image and to aid decision making and foreseeability, these have been attributed to three 'layers of intrusiveness.

| Assessing Non-police originated sources of Watchlist imagery |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                    |         |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------|
|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |         |
| Imagery                                                      | Layer A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Layer B                                                                            | Layer C |
| Image Layer                                                  | Outline                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                    |         |
| Non-police originated image – <b>Layer A</b>                 | <p>Non-police originated images where it is assessed that the public would expect the law enforcement to have access to them (but not including images obtained by covert means) with examples of criteria including:</p> <ul style="list-style-type: none"> <li>• circumstances where images are readily available to the police through open-sources and/or the public have provided information to the police, including but not limited to appeals for information, imagery and footage;</li> <li>• circumstances where the police have obtained the image as a result of a lawful power of search or seizure;</li> <li>• data held by public bodies including where there are information sharing arrangements to support the regular sharing of data or explicit legal powers for information sharing.</li> </ul>                      |                                                                                    |         |
| Non-police originated image – <b>Layer B</b>                 | <p>Images where it is assessed that they raise elevated expectations of privacy or where otherwise obtained covertly without the knowledge of the subject, including any imagery obtained pursuant to:</p> <ul style="list-style-type: none"> <li>• the Regulation of Investigatory Powers Act 2000; and</li> <li>• the Investigatory Powers Act 2016,</li> </ul> <p>where the ability of relevant bodies to obtain such images is further supported and can be anticipated by reference to published Codes of Practice.</p>                                                                                                                                                                                                                                                                                                                 |                                                                                    |         |
| Non-police originated image – <b>Layer C</b>                 | <p>Non-police originated images in circumstances where it is assessed that the public would not typically expect their image to be shared to, or accessed by the police at the point they provided it but there is nevertheless a lawful basis for the police to hold the imagery it has received.</p> <p>To help the public foresee where this may arise, this could include circumstances where the public have shared their image with a controller of data for an explicit purpose (be with a person, business, public body or other third party) and it was not in their contemplation at the time of sharing their image that it may be used for a law enforcement purpose. This would be particularly relevant where the controller promotes an approach to privacy which does not typically collaborate with UK law enforcement.</p> |                                                                                    |         |

6.12 Any non-police originated image should only be included in a Watchlist with the authorisation of the AO where the necessity case to do so is made out. The AO should also consider all the circumstances pertaining to the image and in particular

which layer of intrusiveness the image is attributable to and the factors at paragraph 6.9 above.

- 6.13 The types of non-police originated images that may be deemed appropriate for inclusion within an LFR Watchlist are of people:
- 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 there are reasonable grounds to suspect an individual depicted to be committing an offence; *and/or*
  - c) subject to bail conditions, court order or other restrictions that would be breached if they were at the location at the time of the Deployment; *and/or*
  - d) missing persons deemed increased risk; *and/or*
  - e) presenting a risk of harm to themselves or others; *and/or*
  - f) who are a 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).

#### **Interpretation of Watchlist categories**

- 6.14 **‘Missing persons deemed increased risk.’** This term will be subject to the College of Policing definition of medium risk (or above) contained in Missing Persons APP. That is the risk of harm to the subject or public is assessed as likely but not serious. The harm can apply equally to the subject or any other member of the public.
- ‘Presenting a risk of harm’.** Mitigating the risk of harm will need to have a legal basis for action under a policing common law power. ‘Harm’ can include a risk of harm arising in relation to a person’s welfare and/or a financial harm including as a result of fraud or other dishonesty. It can also include ‘Harm’ in the context of posing a risk to national security.
- 6.15 The risk of harm will be informed by the intelligence case. This will need to inform the AO as to how the individual presents a risk of harm and:
- a) how using LFR to facilitate their location is **necessary** to manage the risk of harm identified; *and*
  - b) why the significance of the harm identified means it is **necessary** for the police to take action in order to manage the risk.
- 6.16 The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

- a) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
- b) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;
- c) how the need to address significance of the harm identified outweighs any expectations of privacy which attach to the Watchlist addition.

**‘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’.** This criteria includes a victim, a person who the police have reasonable grounds to suspect that person would have information of importance and relevance to progress an investigation, or a close associate (partner etc.) of an individual, and that individual who would themselves fall within paragraphs 6.8 (a) – (e) and 6.10 (a) – (e) of the categories that may be deemed appropriate for inclusion within an LFR Watchlist. The threshold for any Watchlist inclusion is high and the use of the category will be by exception; the necessity for inclusion must be based on a specific intelligence-case with the need for the inclusion on a Watchlist being supported by a written rationale. In documenting their rationale, the applicant would need to be able to demonstrate to the AO’s satisfaction:

- a) why the inclusion of each victim, person reasonably suspected of having information, or close associate is **necessary** to help locate the person who is wanted by the courts and/or the police; *and/or*
- b) why locating each victim, person reasonably suspected of having information, or close associate person is **necessary** to advance the policing investigation; *and/or*
- c) why locating each victim, person reasonably suspected of having information, or close associate is **necessary** to ensure their safety and/or the safety of others

6.17 The applicant would also have to demonstrate the **proportionality** of any inclusion on a Watchlist. This would include considering:

- d) any other less intrusive methods and whether they would be viable in the circumstance and what other, more intrusive methods would otherwise be necessary if the addition to the Watchlist is not made; and
- e) the importance of locating the person sought with reference to the threat, harm and risk which the addition to the Watchlist addresses;
- f) expectations of privacy, not least as victims and people with information may have decided not to come forwards to the police. They will also not be the subject of a police investigation themselves and therefore, for any

inclusion on the Watchlist, the information they are believed to have must be assessed to be of significant value to the police or their location is otherwise critical to ensure their safety and/or the safety of others.

- 6.18 The then Surveillance Camera Commissioner recognised the need for policing to locate victims, witnesses and close associates via LFR in his November 2020 guidance, 'Facing the Camera'.<sup>7</sup> In this light, to assist MPS personnel and the wider public understand and foresee how this category may be used, the following are illustrative examples of where the need to add a person to a Watchlist under this category may be made out. In considering these examples, it from a MPS perspective, it is also important to consider any use of LFR in line with the MPS's strategic objectives for LFR.

| Status                                                   | Example Circumstances                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Victim</b>                                            | Intelligence supports an assessment that a victim of crime is under a continuing clear threat to their welfare. Other less intrusive efforts to locate them have failed or are unviable in the time available and there is a need to locate them for their own safety.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Person reasonably suspected of having information</b> | <p>The angle of the only CCTV from a violent gang-related knife attack does not show the faces of the perpetrators who remain at large. The footage does however show the faces of others who are reasonably considered to have seen the attack and it is clear that they should have had a good line of sight of it.</p> <p>If those people who are considered to have seen the offence can be located and they are assessed by the MPS as having relevant information that could be vital to progress the investigation, their location could help bring violent offenders who present a risk to society to justice.</p> |
| <b>Close associate</b>                                   | The MPS has received information that a person wanted for a serious sexual assault has been receiving phone calls from a close associate. They are using public phone boxes to remain in contact and support the perpetrator whilst they hide from the police. MPS has established that the close associate is not residing at their last known address and has been unable to otherwise locate them.                                                                                                                                                                                                                      |

### Additional Watchlist Categories

- 6.19 It may also be appropriate to include Additional Watchlist Categories into a Watchlist, in addition to those included in a Watchlist to meet the primary purpose of the Deployment. These Additional Watchlist Categories can comprise:-

<sup>7</sup> See paragraph 4.49 at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/940386/6.7024\\_SCC\\_Facial\\_recognition\\_report\\_v3\\_WEB.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf)



- a) *Those with outstanding arrest warrants or are otherwise required by the courts within the MPS area.*

The courts have already given consideration as to the necessity to locate this category of persons and given a direction that they should be apprehended. Such people pose a risk to the public in general. In such circumstances, and noting that this is limited to those wanted by the courts within the MPS's area of operation, it is appropriate to consider whether LFR should be used to locate these people.

- b) *Those identified on a case-by-case basis by investigating officers as suitable for inclusion on an LFR Watchlist providing they fall within the criteria at paragraphs 6.8 and/or 6.13 (a)- (f), as applicable.*

In these circumstances, the investigating officer (IO) is best placed to assess the need to locate an individual and why LFR is both necessary and proportionate in the circumstances. The IO will also understand what efforts have been made to locate a particular person, or why other options may not be viable in the circumstances. Where an IO decides to pursue use of LFR, they should record their decision and rationale in writing using systems such as CRIS, Crimint, and Merlin. The IO must contact the LFR operational team to have individuals added to the Watchlist using an MPS LFR Form 2 and ensure that they keep their decision to pursue the use of LFR under review. **When an individual no longer needs to be on a Watchlist, the IO must contact the LFR team to have the individual removed with immediate effect.**

- 6.20 When the AO considers authorising the inclusion of Additional Watchlist Categories, the AO must have regard to the nature of the Deployment when considering Watchlist composition so as to ensure it is not excessive and that the Deployment is one at which there are reasonable grounds to suspect that one or more persons in the Additional Watchlist Category will attend at a time or times at which they are to be sought by means of LFR.

## 7 MPS LFR Documents

- 7.1 **Assessments**; For each authorised LFR operation, the following assessments need to be created, reviewed, and amended where necessary:-
- (i) Data Protection Impact Assessment\* (Review/Amend/Adopt)<sup>8</sup>; *and*
  - (ii) Equality Impact Assessment\* (Review/Amend/Adopt); *and*
  - (iii) Community Impact Assessment\* (carry out); *and*
  - (iv) The Surveillance Camera Commissioner's Self-Assessment\* (Review/Amend/Adopt); *and*
  - (v) LFR Operational Risk Assessment (carry out).

---

<sup>8</sup> The DPO and ILSG's roles start during the planning process continue throughout the LFR Deployment – acting as points of contact and providing means of ongoing assurance in relation to data processing queries.

**Note:** \*Any assessment listed above showing 'Review/Amend/Adopt' has already been created by the MPS LFR team. Each will require a case-by-case consideration to ensure the document remains appropriate and sufficient for each LFR operation. Assessments should remain under continual review to ensure the Deployment falls within them and they remain sufficient for the circumstances as they evolve.

## **8 Risk Assessment & Resource Levels**

- 8.1 Each Deployment should be risk assessed and the appropriate risk assessment documents completed. The anticipated risk to officers and the public should be balanced against the overall intelligence picture, relevant factors linked to persons included on the Watchlist (e.g. seriousness of offences and warning markers linked to the use of violence, carriage of weapons, and propensity to escape, etc), the physical environment surrounding the Deployment, timing, community tension, and any other factors that appear relevant.
- 8.2 The level of resources, including back-up contingencies, required to support each Deployment is a matter to be determined by the operation's command team.
- 8.3 Given the level of intrusion linked to the use of LFR for members of the public passing through the Zone of Recognition, and the processing of biometric data, it is vital that the command team ensure that sufficient resources are available to respond effectively to Alerts and to meet the law enforcement purpose of the LFR Deployment.
- 8.4 LFR System Engineers will be deployed to support LFR Deployments and will come with suitable vehicles where required.
- 8.5 All MPS officers and staff deployed on LFR Deployments must be compliant and in-date with MPS emergency life support (ELS) and officer safety (OST) training requirements. Exceptions to this must be specifically addressed within the written risk assessment. All MPS officers and staff involved in an LFR Deployment must receive LFR training prior to being deployment.

## 9 Planning & Booking

- 9.1 As part of the LFR planning process and before the AO authorises a Deployment, the MPS LFR team (including LFR System Engineers) should be consulted on the appropriateness and viability of a Deployment.

## 10 LFR Operational Roles

### LFR Command Team

- 10.1 LFR Deployments must be supported with a clear command structure. The following roles are defined for the purpose of creating an appropriate hierarchical command structure:-
- a) **Gold Commander (Superintendent or above<sup>9</sup>);** There is only one Gold Commander for any LFR Deployment. Gold has strategic command of the operation and must ensure that their 'strategic intention' aligns with the Written Authority Document and supporting assessments for the Deployment<sup>10</sup>. Gold is to appoint the command team for the Deployment, and to ensure sufficient resources, equipment and personnel will be available to meet their strategic intent for the Deployment. The Gold is to review and adopt the Operational Risk Assessment to ensure that it aligns with their strategic intention for the Deployment.
  - b) Gold maintains overall responsibility for ensuring that the use of LFR remains lawful, necessary and proportionate. Gold will also liaise as necessary with NPCC ranked officers. Gold can also perform the AO role.
  - c) Note: this role is different to the role of MPS SRO for LFR who holds the strategic responsibility for LFR as a capability as opposed to an operational-level responsibility.
  - d) **Silver Commander (Inspector or above);** There is only one Silver Commander for any LFR Deployment. Silver reports to Gold. Silver has tactical command of the Deployment, is responsible for tactical implementation and has front-line responsibility for ensuring compliance with the AO's Authority, the Gold's command and is to monitor the deployment to ensure it stays within the assessments which support the

---

<sup>9</sup> Note that where the urgency criteria (para 4.4) has been applied, the Gold Commander may be of Inspecting rank. However, this should revert to Superintendent or above as soon as a Superintendent reviews the Deployment and provides authorisation for the Deployment to continue.

<sup>10</sup> Assessments comprise the Data Protection Impact Assessment, the Equality Impact Assessment, the Community Impact Assessment and the Operational Risk Assessment.

Deployment<sup>11</sup>. This officer has absolute authority to suspend or terminate the Deployment at their discretion. They are also responsible for ensuring that the use of LFR and their tactical implementation remains lawful, necessary and proportionate throughout the duration of the Deployment, having particular regard to the effectiveness of the safeguards in place whilst LFR is being used.

- e) **Bronze Commander (Sergeant or above);** Bronze Commanders are assigned operational command responsibilities by Silver. Bronze Commanders report to Silver. Bronze Commanders should be present at Deployment locations unless otherwise directed by Silver. There may be more than one Bronze Commander subject to requirements set by Silver. Where this is the case, Silver must document command responsibilities and protocols with sufficient clarity, and ensure that they are fully understood by all officers and staff involved in the Deployment.
- f) **Bronze Community;** Bronze Community is an individual appointed by Silver specifically to oversee and manage community / stakeholder engagement relevant to the LFR Deployment. The Bronze Community should pay particular regard to the Community Impact Assessment.

- 10.2 Where LFR Deployments form part of a larger overarching policing operation, the terms Gold, Silver and Bronze (as described above) may be substituted for alternative command team terminology, or be subsumed into a larger command structure as necessary and appropriate for the effective delivery of the overarching policing operation.

### **LFR Operator**

- 10.3 LFR Operators receive detailed training prior to being deployed operationally. Their role is to monitor and assess system Alerts, before working with LFR Engagement Officers (as necessary) to decide whether an Engagement is required.
- 10.4 The LFR Operator should log all Alerts to help facilitate and support command team reviews during the Deployment, and those that take place post-Deployment. The LFR Operator must flag any concerns they have regarding LFR system performance (be it generally or in relation to specific Watchlist images) to the Silver Commander.
- 10.5 The LFR Operator's log should include:-
  - a) the LFR Operator's assessment of each Alert as part of their assistance to the Engagement Officer when Adjudicating over Alerts prior to making any decision to Engage; *and*
  - b) what decision was taken regarding whether to Engage a member of the public or not; *and*

---

<sup>11</sup> Assessments comprise the Data Protection Impact Assessment, the Equality Impact Assessment, the Community Impact Assessment and the Operational Risk Assessment.

- c) whether an Engagement was successfully undertaken, and the outcome of the Engagement.

### **LFR Engagement Officer**

- 10.6 LFR Engagement Officers must have an understanding of the LFR system, how it performs, and what effect Subject, System, and Environmental Factors might have. These officers must receive a full operational briefing prior to deployment. These officers may be deployed in uniform or plain clothes.
- 10.7 When conducting an Engagement, LFR Engagement Officers must ensure that they do so lawfully, and in an appropriate and proportionate manner. Officers must comply with the Code of Ethics at all times. Wherever possible, members of the public who have been subject of an Engagement, should be supplied with an LFR information leaflet.
- 10.8 The LFR Operator may be supportive of an Engagement taking place, but in any case, it is always for an LFR Engagement Officer to make their own final decision on whether an Engagement should take place<sup>12</sup>. The LFR Engagement Officer should receive an Alert on their handheld device (or otherwise had sight of it) and must then make their own decision about whether they should instigate the Engagement or not. It must not be an automatic consequence that an Alert results in an Engagement. In making their decisions, LFR Engagement Officers must give due regard to the likelihood of Subject, System, or Environmental Factors influencing the generation of an Alert.
- 10.9 When an Engagement is initiated, it is for the officers involved to investigate the identity of the person Engaged using appropriate and lawful means at their disposal.
- 10.10 Whilst officers must exercise their own discretion when using their powers of arrest and detention, MPS policy is that an LFR system-generated Alert on its own, indicating that a person is wanted, should not ordinarily be taken as providing sufficient grounds for arrest or detention. Officers should always seek to make sufficient additional enquiries to satisfy themselves of their grounds to arrest or detain. Where confronted with a non-compliant subject, and the circumstances are such that an officer has an honestly held belief they must use their powers of arrest/detention before further checks have been possible, and this results in the use of those powers, then further checks (as necessary) should be made as soon as is reasonably practicable, so that the decision to arrest/detain is reviewed without unnecessary delay.
- 10.11 If an Engaged individual cannot be identified or fails to confirm their identity, this alone does not constitute a criminal offence and does not necessarily render them

---

<sup>12</sup> The driving force behind this point is that an LFR Operator should not be making the decision that an Engagement Officer carries out an Engagement. Notwithstanding this point, LFR Engagement Officer must still follow lawful orders given by supervisors. It still follows that any officer must form their own 'reasonable grounds of suspicion' (which may rely on information provided by others), and/or have a clear understanding of the legal basis supporting any action they take.

liable to arrest. Officers must be in a position to justify the use of any powers, any action taken, and have a lawful basis for doing so.

- 10.12 After any Engagement (that follows an Alert), the LFR Engagement Officer must update the LFR Operator with the outcome of that Engagement.
- 10.13 Where members of the public choose to exercise their right to avoid an LFR Zone of Recognition, officers are reminded that this is not an offence. The police have no legal powers to direct or compel members of the public to enter a Zone of Recognition. None of this means that LFR Engagement Officers, or other officers involved in an ancillary role linked to an LFR Deployment, 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.

### **LFR System Engineers**

- 10.14 LFR System Engineers have enhanced technical training for the Deployment of LFR (see MPS LFR Policy Document for further information). LFR System Engineers are responsible for the set-up of the LFR equipment and the optimisation of the LFR system to maximise performance.

## **11 Post-Deployment**

- 11.1 Following each LFR Deployment, the Gold Commander must ensure that a post-Deployment evaluation is completed with a Cancellation Report being produced. The evaluation process must capture an assessment of the operational effectiveness of the LFR Deployment. This evaluation should be both *qualitative* and *quantitative* in nature.
- 11.2 The evaluation should clearly articulate what measures are used to assess effectiveness and what benchmarking criteria are used. It should also assess the effectiveness of the safeguards used for the Deployment and what opportunities exist to improve them for future use, and how learning will be shared.
- 11.3 The evaluation may include as many measures as appear appropriate, but as a minimum must include the following metrics (including what methods were used to obtain them):-
  - a) total number of individuals and the total number of images included in the Watchlist (*there may be multiple images of some individuals*); *and*
  - b) total number of facial images detected in the video stream that were of sufficient quality for searching against the Watchlist (i.e. the LFR system was able to generate a Template from them); *and*
  - c) total number of LFR system-generated Alerts; *and*
  - d) total number of Alerts that do not result in an Engagement; *and*

- e) total number of Alerts where a decision was taken to Engage an individual;  
*and*
- f) total number of Alerts that are confirmed as correct (the individual is who the LFR system suggests are); *and*
- g) total number of correct Alerts that result in an Engagement that do not require any further police action; *and*
- h) outcome of each case where police action is instigated following an Alert;  
*and*
- i) number of people Engaged, where the Engagement was not the result of Alert, including the reasons and outcome.

## 12 LFR System Security

12.1 The LFR system includes a number of physical and technical security measures. These include:-

- a) images are transferred onto the LFR system via a USB device using an AES-CBC 256-bit full disk hardware encryption engine; *and*
- b) the LFR system is a closed circuit TV system that implements defences in depth principles to protect the application and related data; *and*
- c) the LFR system is physically protected when in use and securely wiped following each Deployment; *and*
- d) role based access controls with limited user permissions are implemented on the LFR system; *and*
- e) the LFR application is connected to mobile devices using a private access point with three levels of protection; Specific IP addressing, password access to the access point, and password access to the mobile App. The mobile App has a RESTful API and will be covered by SSL; *and*
- f) the Dashboard and RESTful API are secured with SSL and TLS by default; *and*
- g) all connections are directed through HTTPS; *and*
- h) a full audit is maintained of all user initiated actions undertaken during the course of a Deployment; *and*
- i) technical issues with the LFR system are always dealt with by LFR System Engineers deployed on the operation.

## 13 Data Retention & Data Management

- 13.1 The MPS must ensure that the processing of any data associated with LFR is conducted in a lawful way and in compliance with the MPS LFR Documents. This means that:-
- a) where the LFR system does not generate an Alert, that a person's biometric data is immediately automatically deleted; *and*
  - b) the data held on the encrypted USB memory stick used to import the Watchlist is deleted as soon as practicable, and in any case within 24 hours, following the conclusion of the Deployment.
- 13.2 Where the LFR system generates an Alert, all personal data is deleted as soon as practicable and in any case within 31 days, except where:-
- a) personal data is retained in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*
  - b) personal data is retained in accordance with the MPS's complaints / conduct investigation policies.
- 13.3 All CCTV footage generated from LFR Deployments is deleted within 31 days, except where retained:-
- a) in accordance with the Data Protection Act 2018, MOPI and the Criminal Procedures and Investigations Act 1996; *and / or*
  - b) in accordance with the MPS's complaints / conduct investigation policies *and/or*
  - c) in accordance with an approved programme of testing in order to provide for the continued evaluation of the LFR system using operationally realistic data in line with the ongoing nature of the Public Sector Equality Duty - any requirement to retain the CCTV footage for longer than 31 days will be subject to an approved DPIA for such testing and arrangements to ensure data subjects are informed as to the arrangements that will apply to the use and retention of such data.
- 13.4 To support compliance the LFR system has a full audit capability, and the LFR Operator's log is retained in accordance with MOPI.
- 13.5 The loss or theft of any LFR hardware (laptop, mobile device, camera etc.) or other data, irrespective of whether or not protected by encryption, must be reported immediately to the AO, Gold, and the MPS Data Protection Officer.

### **Register of Deployments**

- 13.6 Any Deployment of LFR must be recorded on a centrally held register. This register will record a number of things including:-
- a) name and rank of the AO and command team; and
  - b) date, time, duration, and locality of Deployment; and



- c) Watchlist composition statistics (not including any personal data); and
- d) the number of Alerts and the various statistics relating to these; and
- e) number of Engagements and their results;

13.7 The MPS will make information relating to LFR Deployments available to the public in accordance with the MPS LFR Documents.

## 14 Contact Information

14.1 The MPS LFR team can be contacted using the following email address; LFR@met.police.uk.

## 15 Further Documentation

15.1 Further documentation is available providing useful information relevant to LFR. This is detailed below.

- a) Information Management APP; [www.app.college.police.uk/app-content/information-management](http://www.app.college.police.uk/app-content/information-management) t;
- b) National Decision Model; [www.app.college.police.uk/app-content/national-decision-model](http://www.app.college.police.uk/app-content/national-decision-model) ;
- c) National Intelligence Management; [www.app.college.police.uk/app-content/intelligence-management](http://www.app.college.police.uk/app-content/intelligence-management) ;
- d) College of Policing Code of Ethics; [www.app.college.police.uk/code-of-ethics](http://www.app.college.police.uk/code-of-ethics) ;
- e) Home Office Biometric Strategy – Published June 2018; [www.gov.uk/government/publications/home-office-biometrics-strategy](http://www.gov.uk/government/publications/home-office-biometrics-strategy);