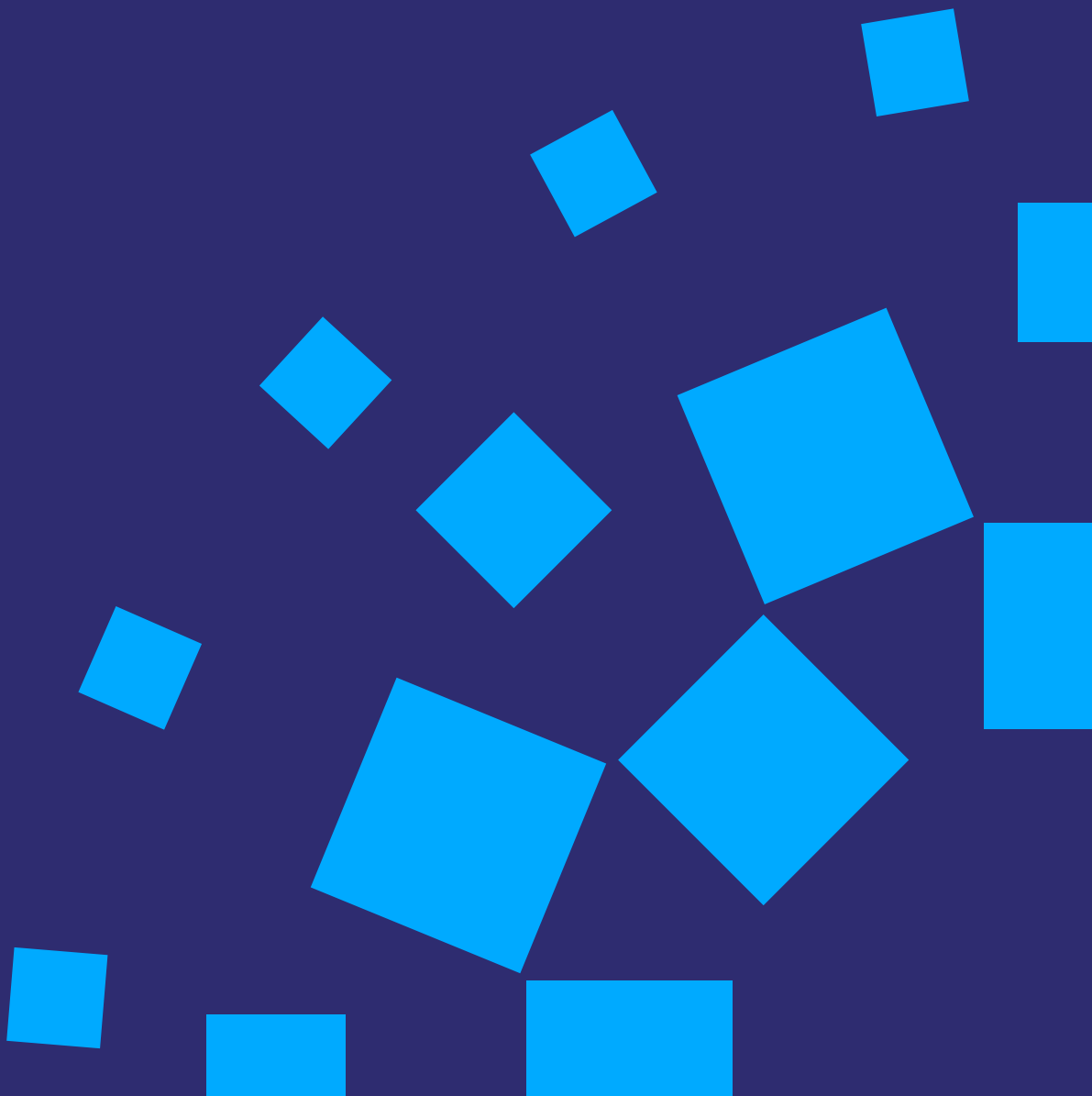
College of Policing

Working together to keep people safe

Authorised Professional Practice Live facial recognition

Consultation

Guidance for the overt deployment of live facial recognition technology to locate persons on a watchlist



If you have any enquiries regarding this publication, please contact us on email **contactus@college.pnn.police.uk**

This document has been created with the intention of making the content accessible to the widest range of people, regardless of disability or impairment. To enquire about having this document provided in an alternative format, please contact us on email **contactus@college.pnn.police.uk**

Contents

1 LFR overview

1.1 Introduction

1.1.1 Live facial recognition (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.

1.1.2 LFR can be a valuable policing tool that helps forces keep the public safe and meet their common law policing duties. These duties include preventing and detecting crime, preserving order and bringing offenders to justice.

1.1.3 The following are illustrative examples where LFR may help forces achieve their 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 (eg, 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 (eg, stalkers, terrorists, missing persons deemed at increased risk[1])

d. supporting the use of targeted preventative policing tactics in areas where intelligence indicates crime may be committed

1.1.4 The technical operation of LFR comprises of the following six stages:

a. **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

1 Refer to paragraph 2.5.2 for further details.

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.

b. **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 provides forces with considerations relevant to the locations where forces may select to deploy cameras when using them for LFR.

c. **Face detection:** Once a CCTV camera used in a live context captures footage, the LFR software detects individual human faces.

d. **Feature extraction:** Taking the detected face, the software automatically extracts facial features from the image, creating the biometric template.

e. **Face comparison:** The LFR software compares the biometric template with those held on the watchlist.

f. **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 acting as an autonomous machine-based process devoid of user input.

1.1.5 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.

1.2 Purpose and scope of the LFR guidance

1.2.1 This APP has been written in a way that is consistent with the '**Facing the camera**' guidance produced by the Surveillance Camera Commissioner (SCC). Chief officers should continue to have regards to the SCC guidance.

1.2.2 The APP aims to:

a. facilitate a national consistency of approach to the overt deployment of LFR technology to locate persons on a watchlist

b. 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

c. 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

d. establish the governance arrangements for the deployment of LFR

1.3 Out of scope

1.3.1 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 probe image for analysis, and is also out of scope for this guidance.

1.3.2 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.

1.3.3 In summary, this guidance does **not** extend to:

a. manually instigated facial recognition for retrospective searching of video or still images

b. human-initiated, near-real-time facial search submitted from a mobile device (or similar)

c. any use of LFR systems operated by a third party, or data sharing for the purpose of facilitating the use of those systems by forces – in such instances, additional privacy considerations would be required (eg, additional information sharing agreements and audit requirements), which are beyond the scope of this guidance

d. any covert use of LFR

1.4 Legal context

1.4.1 This APP has been written to give 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 recent 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.

1.4.2 **Legal framework:** Chief officers with responsibility for deployment of LFR operations will need to satisfy themselves of the legal framework to use it. 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.

1.4.3 Chief officers must 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:

- common law policing duties
- 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

1.4.4 **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 forces in the context of their particular deployment plans and their policy for using LFR, but may include consideration of the following.

a. **Articles 2 (right to life) and 3 (prohibition of torture)**, which may be engaged when an alert has been generated regarding a force's ability to respond to it.

b. **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.

c. **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, 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.

1.4.5 **Force policy documents:** 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.

1.5 Public sector equality duty

1.5.1 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.

1.5.2 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:

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.'

1.5.3 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. A National Institute of Standards and Technology (NIST) report in 2019 concluded that 'some developers supplied identification algorithms for which false positive differentials are **undetectable**'.

1.5.4 Scientific opinion indicates that the accuracy of facial recognition may be influenced by the data sets used to train its capabilities. Specifically, any imbalance in the demographics of the system's training data sets may lead to a similar and corresponding imbalance in the ability of algorithms to assess the biometric characteristics (faces) of those demographics accurately.

1.5.5 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.

1.5.6 Forces should address the PSED through:

a. 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

b. 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

c. ensuring that there is rigorous oversight into 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

d. 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

1.6 Force policy documentation

1.6.1 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:

a. using overt LFR technology in a responsible, transparent, fair and ethical way, in accordance with all relevant law

b. using LFR only when other, less intrusive methods would not achieve the legitimate and lawful policing objectives

c. strengthening and consistently developing LFR technology capability to protect the public, tackle crime, help safeguard vulnerable people and keep communities safe

d. 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 benefits of LFR and explains how issues such as privacy, equality and transparency will be addressed

e. 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

f. 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

g. 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

h. maintaining good operational governance through a command structure that incorporates operational and technical leads for the deployment of LFR, with clear decision making and accountability

i. transparently identifying, managing, and mitigating reputational and organisational risk to the force

j. continuously learning from deployments, identifying lessons to learn from each deployment

k. maintaining the security of both the LFR system and data contained within it

l. liaising with independent regulators where appropriate

m. identifying the metrics against which the success of deployments will be judged, including setting the force's targeted false alert rate in policy

n. continuously assessing the success of deployments against the above metrics, to ensure ongoing proportionality of its use and to provide reassurance regarding the ongoing performance of the technology and algorithms

o. 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 FR technology must be instantaneously (or near instantaneously) and automatically deleted, without need for any human **intervention**

p. ensuring that records of false positive alerts are 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

1.6.2 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 must comply with the requirements set out in paragraphs **1.6.3** to **1.6.5**.

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

a. an imminent threat to life or of serious harm to people or property

b. 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

1.6.4 If an authorisation is given under the urgency criteria above, the information and rationale must 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 must stop.

1.6.5 If a further law enforcement purpose is identified after the AO has issued their authority for an LFR deployment, the AO must 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.

1.7 Supporting policy documentation

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

a. LFR Authorisation Process Guidance Flowchart, or an equivalent document, which clearly sets out the decision-making steps to use LFR.

b. 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

c. Data protection impact assessment (DPIA), 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**.

d. Equality impact assessment (EIA), or a similar document, which enables the force to demonstrate its compliance with the PSED for the types of deployment that the force intends to undertake.

e. Community impact assessment (CIA).

f. 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

g. 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

1.7.2 **Command structure**

1.7.3 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 must 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 separate 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.

1.7.4 **Gold:** In strategic command of force LFR deployments, the force SRO.

1.7.5 **Silver:** The AO for the operation, responsible for the actions in **1.8**.

1.7.6 **Bronze:** The operational commander 'on the ground' overseeing the operation in real time.

1.8 Operational governance, oversight and command structure

1.8.1 **Criteria for deployment**

1.8.2 Each deployment must 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 must then be recorded in writing by the AO as soon as is practicable and, unless urgent, prior to the deployment of LFR.

1.8.3 The deployment must be:

- targeted
- intelligence-led
- time-bound and geographically limited

1.8.4 Force operational documentation

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

1.8.6 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.

1.8.7 Taken together, the LFR application and written authority document must:

a. 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

b. 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

c. 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 need' is
- 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

1.8.8 The following documentation should support each LFR deployment.

Table 1: LFR deployment specific documents and records	
Assessments	These include a CIA, an EIA (or other similar documented record), an overarching DPIA and the SCC's self-assessment. These documents need to be considered by the decision-maker when making an authorisation to ensure that they are sufficient to address the issues arising from the proposed deployment. The decision maker must involve their data protection officer in writing the DPIA and in managing the processing of personal data. The decision-maker must ensure that issues have been adequately identified, documented and mitigated, to ensure that the deployment is both necessary and proportionate to the policing purpose.
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

Table 1: LFR deployment specific documents and records	
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 must be retained in accordance with **Information Management Authorised Professional Practice (APP)** and other relevant legislation or policy, and must be made available for independent inspection and review as required.

Table 1: LFR deployment specific documents and records	
LFR cancellation report	Records details of: ■ where and when a deployment was carried out ■ the circumstances that brought a deployment to a conclusion ■ what resources were used ■ relevant statistics ■ outcomes ■ a summary of any issues following a post-deployment review
Deployment logs	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.

2 Watchlists

2.1 Outline

2.1.1 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 must be approved by the AO, and must be specific to an operation or to a defined policing objective. Watchlists, and any images for inclusion on a watchlist, must also be limited to the categories of image articulated in force policy documents, such as those set out at paragraphs **2.3.1** and **2.4.1** (as applicable). Force policy documents should also provide that the composition of watchlists:

a. is based on the intelligence case

b. is reviewed before each deployment, to ensure that all images meet the necessity and proportionality criteria for inclusion

c. is not excessive for the purpose of the LFR deployment

d. 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

e. must 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 must 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

f. 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 must require an ongoing review of the watchlist, covering the issues of review, retention and deletion

2.2 Specific considerations relating to protected characteristics

2.2.1 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.

2.2.2 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.

a. There may be different privacy expectations around the use of LFR that are particularly relevant in relation to these people, given their potential vulnerability[2].

b. 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

2 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 that 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)**.

a particular protected characteristic. In this regard, the forces should assess whether these persons are particularly susceptible to exploitation and coercion, and should take steps to mitigate any risk arising.

2.2.3 In all cases, force policy documents should require that those undertaking each deployment must 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 relevant disability[3]

2.2.4 In relation to safeguards to address greater expectations of privacy, and given the potential for system factors relating to age, force policy documents should 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.

2.2.5 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, as well as 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 of a suitable quality 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.

3 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 suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing that inhibits their facial features from being recognised.

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.

2.3 Police-originated images that may be included on a watchlist

2.3.1 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:

a. wanted by the courts

b. 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; and/or

c. 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

d. missing persons deemed at increased risk of harm (see paragraph **2.5.1**)

e. presenting a risk of harm to themselves or others (see paragraph **2.5.2**)

f. a victim of – or witness to – an offence, or a close associate of an individual who would fall within paragraphs a-e above (see paragraph **2.5.3**)

2.3.2 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

2.4 Non-police-originated sources of watchlist imagery

2.4.1 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[4]. Non-police-originated images 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 at paragraphs **2.3.2**. The types of non-police-originated images that may be deemed appropriate for inclusion within an LFR watchlist are of people in the categories **2.3.1** (a) to (f) above.

2.5 Interpretation of watchlist categories

2.5.1 **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.

4 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.

2.5.2 **Presenting a risk of harm:** This term will be informed by the intelligence case. This will need to inform the AO as to how:

a. the individual presents a risk of harm

b. using LFR to facilitate their location is necessary to manage the risk of harm identified

c. 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 of other dishonesty. Harm can also arise if a person potentially poses a risk to national security.

2.5.3 **Victim of, or witness to, an offence or close associate of an individual:** This criterion includes a victim or witness, or a close associate of an individual (such as their partner), where that individual would themselves fall within paragraphs **2.3.1** and **2.4.1** (a) to (f) of the categories that may be deemed appropriate for inclusion within an LFR watchlist. The threshold for any watchlist inclusion is high. The necessity for inclusion must be based on a specific intelligence case and supported by a written rationale. In documenting their rationale, the applicant would need to able to demonstrate, to the AO's satisfaction, one or more of the following:

a. why the inclusion of each victim, witness or close associate is necessary to help locate the person who is wanted by the courts and/or the police

b. why locating each victim, witness or close associate is necessary to advance the policing investigation

c. why locating each victim, witness or close associate is necessary to ensure their safety and/or the safety of others

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

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

b. 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.

c. 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.

d. 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 must therefore be assessed to be of significant value to the police, or their location must be otherwise critical to ensure their safety and/or the safety of others.

e. 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.

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

3.1 Measures during an LFR deployment

3.1.1 Force policy documents should provide that signs publicising the use of the technology must be prominently placed in advance outside of the zone of recognition. This measure is to alert members of the public of the presence of LFR technology and to allow them sufficient time to exercise their right not to walk into the zone of recognition.

3.1.2 You should 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).

3.1.3 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.

3.1.4 The AO must define 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 and be capable of being considered and evaluated by an objective third person.

3.2 Privacy considerations relevant to an LFR deployment location

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

a. The reasonable expectations of privacy that the general public may have as a whole at that location:

   i. some places attract greater privacy expectations than others (see **3.2.1 (b)**)

   ii. 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 unduly processing biometric data

b. Whether a proposed deployment location attracts particular concerns, by reference to those expected to be at a particular location[5]. Where it is practicable to identify a person as being responsible for a proposed deployment location, and 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:

   i. hospitals

   ii. places of worship

   iii. centres for legal advice

   iv. polling stations

   v. schools (and other places particularly frequented by children)

5 If a deployment is necessary at a site that is focused on children (for example, outside a school) 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 (as applicable) who may pass through the zone of recognition. When assessing if 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.

vi. care homes

vii. assemblies or demonstrations

3.2.2 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.

3.2.3 **Oversight bodies and regulatory framework**

3.2.4 Chief officers must 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 also seek to engage with ethics committees, which may meaningfully be consulted in the first instance to help determine relevant oversight arrangements.

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

3.2.6 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.

3.2.7 Summary of National Police Chiefs' Council (NPCC) governance arrangements. Currently under revision.

3.2.8 Other regulatory bodies:

a. **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. This guidance document seeks to apply those principles.

b. **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 DPIA must comply with sections 35-40 (principles 1-6) and section 64 of the DPA 2018, and should be shared with the ICO.

c. **Her 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.

4 Key performance metrics

4.1.1 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 must 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 know their algorithm, given algorithm-specific variation. While publicly available test data from NIST can inform owners, it will usually be informative to measure accuracy of the specific operational algorithm on the operational image data sets.

4.1.2 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. These are detailed in the paragraphs below.

4.1.3 **True recognition rate (TRR):** This is also referred to as the true positive identification rate.

4.1.4 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 when these individuals passed through the zone of recognition (regardless of whether an alert is generated).

4.1.5 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.

4.1.6 **False alert rate (FAR):** This is also referred to as false positive identification rate.

4.1.7 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.

4.1.8 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.

4.1.9 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 on behalf of the force.

4.1.10 **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.

4.1.11 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.

5 LFR terminology

5.1 Outline and scope

5.1.1 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.

5.1.2 **Scope:** The section 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.

5.1.3 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.

5.2 Terminology

5.2.1 **Adjudication**

5.2.2 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.

5.2.3 **Administrator**

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

5.2.5 **Alerts**

5.2.6 **Alert**

5.2.7 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.

5.2.8 **True alert**

5.2.9 When it is determined that the probe image is the same as the candidate image in the watchlist.

5.2.10 **Confirmed true alert**

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

5.2.12 **True recognition rate (TRR)**

5.2.13 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).

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

5.2.15 **False alert**

5.2.16 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.

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

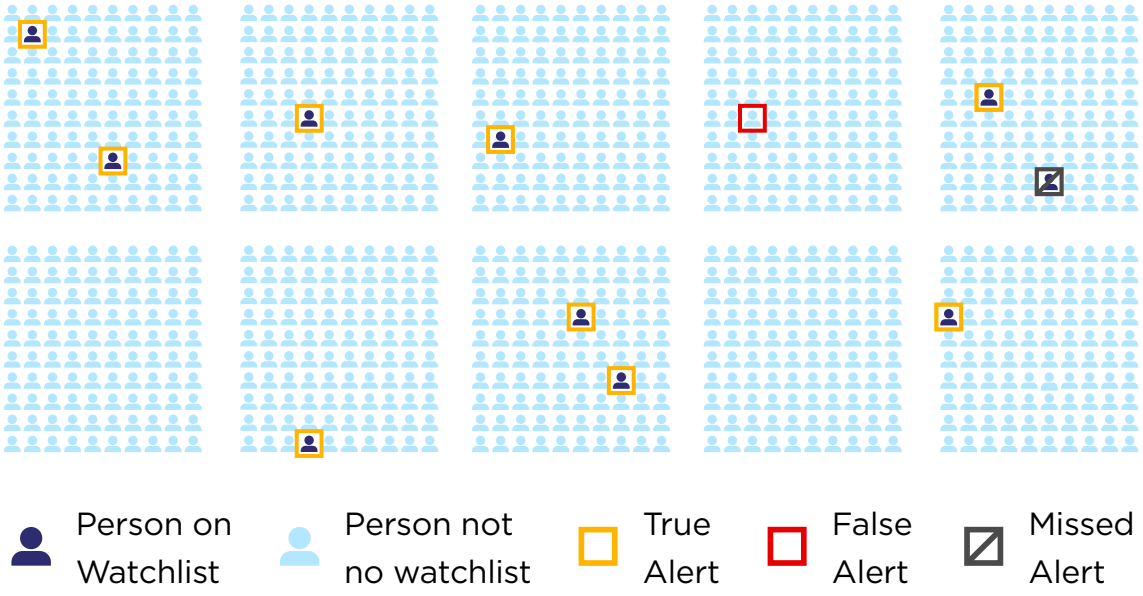
5.2.18 **Confirmed false alert**

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

5.2.20 **False alert rate (FAR)**

5.2.21 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.

5.2.22 This is also referred to as false positive identification rate.



5.2.23 **Application accuracy**

5.2.24 There is no single figure that can determine the accuracy of an LFR application. 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.

5.2.25 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.

5.2.26 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.

5.2.27 **Authorising officer (AO)**

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

5.2.29 **Biometric template**

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

5.2.31 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.

5.2.32 **Blue Watchlist**

5.2.33 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.

5.2.34 **Candidate image**

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

5.2.36 **Deployment**

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

5.2.38 **Deployment record**

5.2.39 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

5.2.40 **Environmental factors**

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

5.2.42 **Faces per frame**

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

5.2.44 **Facial recognition**

5.2.45 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).

5.2.46 **False negative (missed alert)**

5.2.47 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.

5.2.48 **Live facial recognition (LFR)**

5.2.49 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.

5.2.50 **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.

5.2.51 **LFR operator**

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

5.2.53 **Person(s) of interest**

5.2.54 This term comprises persons on a watchlist.

5.2.55 **Probe image**

5.2.56 A facial image that is searched against a watchlist.

5.2.57 **Retrospective facial recognition (RFR)**

5.2.58 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.

5.2.59 **Subject factor**

5.2.60 A factor linked to the individual, such as:

a. demographic factors

b. wearing a head covering

c. smoking

d. eating

e. looking down at the time of passing the camera

5.2.61 **System factor**

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

5.2.63 **Threshold**

5.2.64 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.

5.2.65 **Urgency**

5.2.66 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

5.2.67 **Watchlist**

5.2.68 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.

5.2.69 **Zone of recognition**

5.2.70 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.

About the College

We're the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

college.police.uk

Follow us
@CollegeofPolice

C67I0521