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

Assessments	These include a CIA, an EIA (or other similar documented record), a DPIA and the SCC's self-assessment. 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. 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. Documents such as the DPIA and EIA may be applicable across a number of deployments and, while they will need ongoing to review to ensure sufficiency, they may not need revising for each deployment.

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	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 statistic • 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.
Register deployments	Forces should keep a register of all LFR deployments, which should be published.

Appendix A

Legal framework and governance.

Appendix B

LFR summary process.

Tags

Digital intelligence and investigation