Where – date, time, duration and location of deployment

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

First published 22 March 2022 Updated 27 July 2023
Written by College of Policing
3 mins read

Measures during an LFR deployment

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

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

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

Privacy considerations relevant to an LFR deployment location

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

- The reasonable expectations of privacy that the general public may have as a whole at that location:
  - some places attract greater privacy expectations than others
  - the number of cameras used actively by the LFR system should also be considered in this context, to ensure that the size and scale of the deployment enables those on a watchlist to be effectively located without unnecessarily processing biometric data

- Whether a proposed deployment location attracts particular concerns, by reference to those expected to be at a particular location. Where it is practicable to identify a member of the community as being responsible for a proposed deployment location (for example, outside a place of worship). Where that location raises a greater expectation of privacy, consideration should be given to liaising with that person as part of a community impact assessment process. Legal advice should be sought where appropriate. Examples where those who attend may have a greater expectation of privacy, feel less able to express their views or otherwise be more reluctant to be in the area include:
  - hospitals
  - places of worship
  - centres for legal advice
  - polling stations
  - schools (and other places particularly frequented by children)
  - care homes
  - assemblies or demonstrations

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

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

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

Oversight bodies and regulatory frameworks

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

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

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

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

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

Other regulatory bodies

Biometrics and Surveillance Camera Commissioner (BSCC)

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

Information Commissioner's Office (ICO)

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

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

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

Tags

Digital intelligence and investigation