Norfolk and Suffolk Constabularies' Live Facial Recognition (LFR) Legal Mandate

Title: Outlines the legal basis for Norfolk and Suffolk Constabularies' use of overt LFR technology to locate persons on a Watchlist

Policy Reference Number:

Procedure(s) Reference Number:

Version Number: 6.0

Senior Officer Lead: C/Supt Mears

Author: A/Sgt Dominic Mason

Index

Terms and Definitions:

Capitalised terms used in this Norfolk and Suffolk Constabularies' (together 'the constabularies') LFR Legal Mandate shall have the meaning given to them in the Constabularies' Live Facial Recognition Policy Document unless otherwise defined in the LFR Mandate.

1. Introduction

1.1 Live Facial Recognition (LFR) for law enforcement purposes is not subject to dedicated primary legislation. LFR, like many Police activities, is regulated by a number of different sources such as the common law, primary and secondary legislation as well as both national and local policy. This 'tapestry' of legislation combines to provide a multi-layered legal structure to use and regulate the use of LFR.

Tier one: Legislation

Legal Power to use LFR

a) Common Law

b) Police and Criminal Evidence Act 1984 Code D (revised)

Regulating the use of LFR

Operational & Data Management

c) Human Rights Act 1998

d) Equality Act 2010

e) Data Protection Act 2018 (especially Part 3)

f) UK General Data Protection Regulation

g) Protection of Freedoms Act 2012

Requests for Information in relation to LFR

h) Freedom of Information Act 2000

i) Data Protection Act 2018 (Subject Access Requests)

Tier Two: Code and Guidance

Regulating the use of LFR

a) Surveillance Camera Code of Practice (Amended 2021)

b) Guidance issued by the Surveillance Camera Commissioner (Facing the Camera) (Published November 2020)

c) Associated guidance issued by the Information Commissioner

Tier Three: The Constabularies' LFR Documents

Regulating the use of LFR

a) Live Facial Recognition - Policy Document

b) Live Facial Recognition - Procedures Document

c) Live Facial Recognition - Data Protection Impact Assessments

d) Live Facial Recognition - Equality Impact Assessment

e) Live Facial Recognition - Legal Mandate

2. Common Law

2.1 The police have a number of long-established policing responsibilities and powers derived from common law which have been recognised by the courts. The Constabularies are each obliged to comply with common law and statutory safeguards in delivering their policing operational duties and they rely on common law powers to discharge a number of their duties.

2.2 Key common law powers the Constabularies may rely on when utilising LFR technology include the policing common law powers relating to acts to:

- Protect life and property;
- Preserve order and prevent threats to public security;
- Prevent and detect crime;
- Bring offenders to justice; and
- Uphold national security.

For example, LFR might be deployed in an area impacted with a significant amount of violent crime and running a watchlist of persons who are wanted for arrest for serious violence. The intent being to identify and promptly locate wanted individuals at the earliest stage possible thereby supporting the bringing of offenders to justice but also potentially preventing any violent disorder such individuals may have gone on to cause in that area (and thereby preventing crime, protecting life/property and preserving order).

2.3 The use of common law powers as a legal basis to support the deployment of LFR has been considered and recognised in the 'Bridges' case both in the:

a) High Court Bridges Decision;[1] *and* then on appeal in,

b) Court of Appeal Bridges Decision.[2]

2.4 The Court of Appeal further summarised the legal basis in relation to compilation of Watchlists as being "both authorised under the Police and Criminal Evidence Act 1984 and within the powers of police at common law." The Court of Appeal[3] notes that:

"it is now common ground that SWP do have the power to deploy [LFR]."

[1] R (on the application of Edward Bridges) v The Chief Constable of South Wales Police (SWP) [2019] EWHC 2341 (Admin) (the "High Court Bridges" decision)
[2] R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision)
[3] R (on the application of Edward Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 (the "Court of Appeal Bridges" decision) at [38] (via www.judicary.uk)

Authorising Officers: When considering the use of LFR technology, it must be clear as to the common law policing power or powers that is/are being relied upon in each instance for lawfully authorising the use of LFR. Consider the specific context the deployment will take place in and, if satisfied the power applies, then record all of this as part of the decision-making process.

3. Police and Criminal Evidence Act 1984

3.1 Section 64A of PACE allows the photographing of a person who is detained at a station. It is likely that where LFR is used, the primary source of photographs used to create biometric templates for use in a watchlist will be photographs sourced from records originally created using s.64A of PACE.

3.2 Section 64ZN allows for the photographs to be used for the prevention and detection of crime, the investigation of offences or the conduct of prosecutions. Officers must therefore satisfy themselves when using such images that the purpose of using them in any particular deployment meets one or more of these permitted use cases.

4. Human Rights Act 1998

4.1 The Constabularies' use of LFR must be in compliance with the Human Rights Act 1998. The deployment of LFR technology by the constabularies engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

'There shall be no interference by a public authority with the exercise of the right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

4.2 As a qualified right, any interference with an individual's Article 8 rights is only permissible if:

- There is a legal basis for the interference with the qualified right that the public can understand;
- The activity creating the interference (e.g. the use of LFR) seeks to achieve a legitimate aim;
- It is necessary for the purposes of that aim in a democratic society, and
- The activity creating the interference (e.g. the use of LFR) is proportionate to the legitimate aim being sought.

4.3 It is well-established that the reach of Article 8 can be broad. The case of *S and Marper v. United Kingdom* confirms that Article 8 can be engaged in relation to biometric data and any storing of data relating to it.[4]

4.4 That case recognised that, as regards the processing of personal data in the form of biometric processing in the law enforcement context, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".[5]

4.5 The High Court and Court of Appeal Bridges cases considered Article 8, specifically in the context of LFR technology and confirmed that Article 8 is engaged in so far as someone passes through the Zone of Recognition and in so far as someone is placed on a LFR Watchlist for a deployment. Depending on the nature of the deployment, the then Surveillance Camera Commissioner identified that there are also potential impacts on other human rights. These include the right to freedom of assembly, freedom of thought, belief and religion, freedom of expression, freedom of association, and the protection of discrimination in respect of those rights and freedoms.

Authorising Officers must consider the specific context of each deployment as to whether other rights may be engaged (such as where LFR is proposed to be deployed on the route of a proposed demonstration march and so might engage free speech and association rights, or where a deployment covers the entrance to a place of worship). Authorising Officers should contact Legal Services if they consider a proposed deployment may have a wider human rights point to consider

<u>There is a legal basis for the interference with the qualified right that the public can understand.</u>

4.6 LFR will be used to allow the Constabularies to discharge their well-established operational duties pursuant to common law. The courts have recognised that when considering a potentially legitimate interference with a right the legal basis relied on for that legitimate interference "need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them".[6]

4.7 In the case of *R (Catt) v Chief Police Officers [2015] UKSC 9*, Lord Sumption recognised that the police can lawfully process the personal data of individuals by recording and retaining it where it is in accordance with the law, for police purposes and proportional. In that case the information primarily concerned personal information that was obtained and recorded in the context of a person being present at events in publicly accessible space (as would be the case as regards the live non-watchlist data processed at a LFR deployment). The court recognised the police's common law powers to collect and store information are subject to an "intensive regime of statutory and administrative regulation" under the Data

[4] (2009) 48 EHRR 50, at [66 and 67]
[5] S and Marper v the United Kingdom (2008) at [104] (30562/04 30566/04 via hudoc.echr)
[6] R (Catt) v Association of Chief Police Officers [2015] UKSC 9 at [11].

Protection Act (as well as other legislation) and various guidance documents on the management of police information.

4.8 The courts have further recognised the right of the police to make use of a photograph of an individual. Established purposes include the prevention and detection of crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large as well other a non-law enforcement purposes such as assisting in locating missing persons (with such processing taking place under the UK GDPR regime). It is well established that the reasonable and proportionate use of pictures is allowed for (and justifiable) when pursuing such purposes and will often be of particular value when trying to locate particular persons.

4.9 In the case of the Constabularies' use of LFR, this document outlines the legal basis for any interference with an individual's Article 8 rights. The High Court Bridges case confirmed the police's common law policing powers to be "*amply sufficient*" in relation to this type of use of LFR and confirmed that "*the police do not need new express statutory powers for this purpose*".[7] This was further considered in the Court of Appeal Bridges case which also recognised the sufficiency of the legal framework, noting:

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

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

"be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependant on the will of those who apply it, rather than on the law itself". [9]

4.10 In considering accessibility and foreseeability, the Court of Appeal considered the level of discretion that South Wales Police officers held in the case before it to determine where they deployed facial recognition technology and who they deployed it to locate (i.e. those put on a Watchlist for a deployment). The court refers to this as the "Where Question" and the "Who Question" respectively.

The 'Who' Question:

4.11 When considering how the 'Who Question' should be answered, the Court of Appeal made it clear that, the law does not seek to require that to be accessible persons should get specific confirmation as to who is on a Watchlist (they recognise the Neither Confirm Nor Deny principle)[10]. The Court of Appeal recognised that individuals could be added to a Watchlist for any valid law

[7] R v The Chief Constable of South Wales Police (SWP) [2019] EWHC 2341 (Admin) at [78]
[8] R v The Chief Constable of South Wales Police [2020] EWCA Civ 1058 at [69]
[9] Ibid at [80(2)]
[10] Ibid at [95].

enforcement or other policing purpose where it is fair, proportionate and appropriate to do so. This could be on the basis that they fall within a category such as 'persons wanted on suspicion of an offence', or 'persons wanted on warrant' or are 'vulnerable persons who need to be located'.

4.12 Whilst it is clear the 'who' question can be satisfied on the basis of categories rather than requiring the specific name of every individual, the Court of Appeal is very clear that there are limits to this and that the policies in place must sufficiently set the terms of the discretion applied. In particular, the Court explained why a category of "other persons where intelligence is required" was overly broad and indeterminate such that it is not sufficiently accessible and foreseeable to meet the 'in accordance with the law' test. They noted that the category was not readily understood, nor was it objective – it left "too broad a discretion vested in the individual police officer to decide who should go onto the watchlist" – essentially it allowed police officers to decide what 'other persons where intelligence is required' meant on a case-by-case basis rather than deciding if a subject met the criteria set out in the force policy and whether the subject was appropriate in the context of all the relevant circumstances of the deployment (because for example there is no reason to believe that the subject might possibly be at the location of the deployment).

4.13 Following an approach recognised by the Court of Appeal,[11] the Constabularies address the 'Who Question' in their published LFR Documents, particularly at Section 6 of the Force Procedure. The Constabularies set the foundation criteria that apply to govern the images that may be included on a Watchlist and in what circumstances. It sets out the substantive standard required for inclusion on a Watchlist, linking the necessity and criteria for the inclusion on a Watchlist with the policing need and the proportionality of taking any action looked at in the context of the specific circumstances of the deployment.

***The 'Where' Question**:*

4.14 The Court of Appeal noted that the South Wales Police team "was not able to draw to our attention anything which specifies where AFR Locate may be deployed". The Constabularies' LFR Documents seek to provide comprehensive answers to this question, particularly at Section 3.6 of the Force Procedure.

4.15 In many instances, the underlying need to locate a person will often determine where it is best to site LFR to facilitate making a successful location. For example, a deployment focused on locating those wanted in relation to football violence will naturally often give rise to a location that is connected to such activity such as a football match. However, other factors will also be relevant, and these include the nature of the site itself from a privacy perspective, the kinds of person expected to be passing the site, and the policing need to be at the site (including for the public's protection, supressing crime hotspots, and getting ahead of crime trends). Context will also always need to be considered. Continuing the example, including persons on a watchlist that are associated with one or other of the teams playing at a stadium will likely be justifiable but including another person wanted for football violence but who is a person that is solely connected to some other team (many miles away) is unlikely to be (without the presence of additional intelligence that

[11] Ibid at [118]

specifically links them to potentially appearing at the location of the proposed deployment).

4.16 The Constabularies' have, in developing the published documentation to support the use of LFR, taken close account of the relevant judicial decisions in order to make provision that allows the LFR Legal Framework principles to be predictably applied to the use of LFR in an accessible and understandable way. It allows the public passing through or about to enter an LFR system and those who may be placed on a Watchlist to understand the standards the Constabularies operate to and within, including setting out the authorisation process and requirements to deploy LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

The use of LFR seeks to achieve a legitimate aim

4.17 Article 8 recognises that action taken in the interests of national security, public safety and the prevention of disorder and crime can be legitimate aims. Deployment of LFR in the law enforcement context will always be in support of one or more of those aims, such as the use of LFR in the context of assisting the Constabularies achieve their law enforcement purpose of preventing crime by reducing and investigating violence through the LFR expedited locating of violent offenders. In relation to LFR use for UK GDPR processing such as the location of vulnerable missing persons this would comply with the recognised Art.8(2) aim of the protection of the rights and freedoms of others.

4.18 The means by which the Constabularies may use LFR will be an operational decision within the parameters of the law and the Constabularies' LFR Documents. It will need to be driven by the policing issue at hand. This may vary from the need to locate those wanted in connection with criminality or who otherwise pose a risk of harm, to more preventative tactics designed to bring reassurance to communities and enable the use of precision technology to more proactively focus policing resources, such as the deployment of an LFR system close to a school and using a watchlist made up of sexual offenders who are subject to court orders prohibiting them from being within the relevant distance of a school.

Authorising Officers: At the point it is decided to deploy LFR, the decision maker must be clear as to its purpose and how using LFR will help the Constabularies realise a legitimate aim. In deciding if the use of LFR is a suitable way to achieve that legitimate aim, the decision maker must consider if the benefits of using LFR justify its use for the legitimate aim when compared to any impact on any of the relevant individual's Article 8 Rights and whether there are any other ways to achieve that same aim in a way that poses less interference.

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

4.19 LFR will be used in response to a pressing social need such as by helping the Constabularies combat crime in areas where LFR has the greatest potential to assist. It is a tool that helps the Constabularies to discharge its operational responsibilities, primarily to help prevent and detect crime and protect the most vulnerable.

Authorising Officers: When considering the deployment of LFR, its use is to be underpinned in each specific deployment by an intelligence case which identifies the need to combat the relevant crime or public safety issue or policing need to deploy, and how that relates to the specific deployment (noting that a single deployment may seek to address more than one such need e.g. where both a watchlist for those subject to arrest warrants and a watchlist for locating missing vulnerable persons are run simultaneously). Having identified a need, this will allow the Authorising Officer to consider the use of LFR. Authorising Officers must decide the use of LFR is necessary, and not just desirable, to enable the Constabularies to achieve their identified legitimate aim. In deciding the use of LFR technology to be necessary, the Authorising Officers will document the specific issue which LFR was intending to address and how LFR would be deployed to address that problem (e.g. an issue of outstanding arrest warrants for football-related violence, which is sought to be addressed by using LFR at a relevant football match on the basis that there is a reasonable prospect of the wanted individuals may attend and be identified and located for purposes of arrest). Additionally Authorising Officers must consider whether the deployment was necessary in terms of whether the same result could be achieved in another more proportionate way or not for each purpose.

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

Violence

4.21 The use of LFR will assist the Constabularies in tackling violence. LFR could be deployed (based on intelligence and analysis) to areas of the county in which violence is high and continues to be high despite Police intervention. LFR will assist by allowing the Constabularies to locate those suspected of violent offences that are subject to being arrested on sight within that policing area. The arrest of these outstanding suspects along with the deterrent effect of LFR deployments contributes to the legitimate aim of public safety by reducing the risk of further violence or disorder being committed by those suspects and others. It also at the same time contributes to the protections of the rights and freedoms of others that might otherwise become victims. Additionally, it contributes to the prevention of crime and disorder by facilitating the law enforcement process in locating and allowing for the arrest of individuals subject to potential prosecution of previous crimes which in turn limits the potential for further offending by such persons.

4.22 Additionally, in a climate where police forces need to operate efficiently, the Constabularies have also identified that technology such as LFR can assist with the challenges of quickly and cost efficiently locating those with outstanding warrants or who have otherwise breached their bail conditions compared to (or in addition to) existing methods focused on recognition of wanted individuals by individual police officers or searches of specific locations at specific times. It is right and appropriate to bring those who are unlawfully at large to justice noting the need to protect the public in such circumstances and the ongoing potential threat such persons pose whilst they remain at large and unaccounted for.

4.23 The High Court Bridges case supports this position in that it states "*by including all those who were wanted on warrant there was, potentially, a considerable additional benefit to the public interest*"[12] for a deployment of LFR, given that such persons are arrestable on sight wherever they may be and so providing there is a reasonable possibility the wanted individual might potentially appear at the location it is appropriate to include them on the watchlist even when there is no specific intelligence guaranteeing that they will be in the area of the deployment. The inclusion of wanted individuals into the watchlist in no way increases the intrusion to those passing the system, but (i) the potential to protect the public from those wanted by the courts, and (ii) the positive results into progressing prosecutions and alike as a result of individuals being identified and arrested from use of LFR (especially where other methods of location have failed) justifies the inclusion of those with outstanding warrants as a necessary action to bring offenders to justice and prevent further crime, disorder and harm to others.

The use of LFR is proportionate to legitimate aim being sought

4.24 When considering the deployment of LFR, it is essential that use of this technology is not disproportionate or arbitrary in nature. In this respect the Surveillance Camera Commissioner recognises that:

"used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need".[13]

4.25 In this respect, the following (although not limited to depending on the nature of the deployment) will guide Authorising Officers: the use of LFR should be a reasonable use of the Constabularies' powers - it will not be proportionate if the proposed use of LFR is excessive in the overall circumstances of the investigation, operation or wider operational strategy to tackle a policing issue. All aspects of a deployment must be considered against this principle in particular including whether the size and nature of the watchlist is reasonable and proportionate against the stated aims of the deployment, as well as whether the location and timing of the deployment is appropriate given the aims and the makeup of the watchlist. Officers must take care never to simply reuse watchlists or other operational decisions in relation to deployments, they must be content each time that the use is reasonable and proportionate and that may require the tailoring, adjustment or entire replacement of previous similar deployment decisions to reflect the context of the next one proposed.

4.26 Authorising Officers will need to consider the seriousness of the policing issues at hand and the potential benefits of using LFR and balance this with any wider impact its deployment may have to those on a Watchlist and the public at large. This will allow a decision to be made as to whether LFR is appropriate for use. Authorising Officers must give consideration to the composition of the Watchlist compiled for the LFR system to match against, to ensure that it is not compiled in an excessive or otherwise inappropriate manner. The Watchlist needs to satisfy the necessity and proportionality test and will therefore be driven by the intelligence

[12] At [102]
[13] Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012 at [2.1]

case and therefore be considered on a bespoke basis for each deployment of LFR to ensure it meets the aims of each deployment (Nothing absolutely prohibits two deployments having identical watchlists providing that each was considered and justified on a bespoke basis taking account the relevant context of each specific deployment. Coincidental duplication can happen). It is also important to remember that proportionality isn't a one-way consideration. For example, where a large number of individuals are all sought at once and are believed to be at a particular location, say a demonstration march where it is thought likely that 200 persons all suspected of public order offences at a previous demonstration will again be in attendance. Then deployment of an LFR system to rapidly and comprehensively search for these individuals using a single closed system, is arguably significantly less of an interference than the alternative of providing every one of the 100's of officers on duty at the demonstration with an identity sheet containing the facial images of all 200 wanted individuals. It is also a safer approach in terms of the risk of inadvertent disclosure or other risks.

4.27 With this in mind, the Watchlist compiled for each deployment of LFR should be current; and care must be taken to ensure that it is based on those currently of interest to the Constabularies and/or wider UK law enforcement to mitigate the risk of the LFR system matching with those no longer of interest.

a) Consideration should be given as to the extent of any proposed interference with privacy against what is sought to be achieved and if there are other viable methods to achieve the aim which involve a lower level of interference. A potential challenge to the necessity of including a person on a watchlist in order to locate them will be whether or not other less intrusive but arguably effective methods have been used previously. For example, in some cases this might be whether it is reasonable in the specific circumstances that the individual's last known address has been checked in person first. However, in some instances it may be the case that the use of LFR has a lower interference with privacy compared to other policing tactics. For example, using ANPR, financial enquiries, communications data enquiries, all of which will very likely have a degree of collateral intrusion often involving and providing knowledge to third parties and therefore a potentially higher level of interference with privacy compared to the use of LFR which is more passive and self-contained in nature.

b) This consideration around the extent of any proposed interference with privacy against what is sought to be achieved is considered by the Authorising Officer in setting the criteria for individuals to be included on the watchlist, with each criteria having to be justified and therefore the proportionality of the proposed interference is considered against the legitimate policing aim carefully and in a measured way for each deployment (and in relation to each individual sought to be added to the watchlist).

c) The delayed availability of LFR allows for usual police tactics and potentially less intrusive enquiries to take place first. If those are successful the individuals concerned will then not become eligible to be added to the watchlist, but of course they will remain wanted if those enquiries fail and so would become eligible for entry on the watchlist. Checks of data quality to ensure accuracy and suitability for inclusion based on the criteria as laid out in the authority will take place. Similarly, Category C warrants may not be included on the watchlist

as these relate to 'other warrants' such as all other summary offences, disqualified driving, drunk and disorderly behaviour, prostitution, low level public order and Public Order S5 offences. Given the comparatively reduced seriousness of such offences, it is more likely that the proposed interference of privacy by LFR is not proportionate against what is being sought through the legitimate policing aim. Consequently, unless other additional factors are present it is less likely that such wanted persons are included on the watchlist. To be included, such a case would need to be justifiable and considered by the Authorising Officer based on the specific deployment circumstances.

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

4.29 **Example**:

4.30 Circulating a wanted image in the media may be considered as an alternative to the use of LFR to locate an individual. The use of LFR can be targeted to a specific area and does not result in any of the public being made aware of the identity of a person being sought by the Constabularies (whereas circulation in the media will spread this knowledge to the readership and even wider by secondary word of mouth). It will also be used for a limited period, targeted, based on wider intelligence, restricted to times and places when it is reasonable to expected that a deployment could successfully result in the location of one or more of the individuals sought. By comparison, using the method of disclosing a wanted image to the media results in that person's image being put into the public domain in a less targeted way (both geographically and substantively) and for potentially an indefinite period. Once released, the image is public, and the Constabularies no longer have control of that image. It therefore has potential to remain online even when the person has been traced and thus very likely amounts to a greater intrusion into the privacy of the individual being sought and may also pose a threat to whether or not such an individual can receive a fair trial. Additionally, the publication in the media to the world at large is uncontrolled and so can be less effective than LFR. This is because in the media the image will not just be seen by those seeking to aid the police in locating the individual. But may also be seen and used by persons to further frustrate the purpose of the disclosure (i.e. location of the individual) because associates or family of the individual become aware and then take action to 'tip-off' or otherwise help the individual remain hidden. Because LFR deployments involve no disclosure outside of the relevant police force such compound risks do not exist and so it is arguably more effective at achieving the purpose of locating such individuals. Lastly it is also worth noting that LFR operates in a way where by the resources and activity needed to seek to locate one individual differs very little from that needed when seeking to locate a 1000 people. The same cannot be said of other non-LFR location methods. Some, such as circulation in the media will never practically be an alternative option for 1000 persons at a time, similarly physically searching last known addresses will often be effective but not always so and the method is considerably more resource intensive. The Authorising Officer considering the use of LFR should balance any

intrusion into privacy against the need for the investigative activity. If the Authorising Officer uses LFR in a way which minimises any impact it may have on a person's privacy as far as possible, it may offer a more appropriate, less intrusive alternative to other options. The crucial question the Authorising Officer must satisfy themselves of each time is whether there is another viable method to achieve the relevant aim that involves less interference. Media campaigns are often likely to involve greater degrees of interference but there are other methods that may be available to the police such as doorstep checks that may present a lower overall level of interference dependent of circumstances (and so the Authorising Officer will need to consider whether these should be pursued first or whether in the circumstances such methods are unlikely to be viable because for example there is no known address to check or there is good reason to believe it is highly unlikely that the individual will be at that address because it is out of date or is the scene of the crime etc).

Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record in summary form what other methods, as appropriate, were either not implemented because there were assessed to be insufficient, or inappropriate to fulfil the Constabularies aim or were employed first unsuccessfully.

4.31 All uses of LFR under this Legal Mandate will be overt. In particular this means that there will be public media releases prior to the deployment detailing the date and location of the deployment, the vehicles with the LFR technology are overtly marked police vehicles with signs at (or just beyond) the limit point of the cameras advising the public that they will enter the zone of recognition if they continue in that direction (such signs must always be visible at a distance that allows individuals to take action to avoid the zone of recognition). LFR will be used for a limited time, with a limited footprint, with a defined purpose (controlled in line with the requirements of the Constabularies' LFR Documents). The LFR system will be visibly deployed in an open and transparent way. Consistent with the principle of engaging with the public, the Constabularies' LFR Documents also provide a structure for awareness measures which respond to the nature and objectives of the use of LFR.

Proportionality Controls

4.32 Controls are also designed into the LFR system and its operation to help minimise any impact on the public and those placed on a Watchlist as follows:

a) LFR cannot be used to locate persons unless they have, in advance of the deployment, been included on a Watchlist. Generally, adding individuals during a live deployment is prohibited to provide a process that is designed to ensure to the highest degree possible that proper scrutiny and safeguards are applied when creating a watchlist. It is only right and proper that this is the default position ensuring that the highest scrutiny levels will have been applied to all of the individuals on any particular watchlist save exceptionally where in justifiable particular circumstances an individual may be added on an emergency basis and is subject to reduced process requirements. Alternate provision has been made that will allow for individuals to be included after the usual process has already completed (i.e. during the live

deployment for example) whilst still ensuring appropriate scrutiny and safeguards are applied.

(I) One exception to the standard process would be in cases of such severe threat, harm or risk that it justifies adding of previously unincluded persons, for example, in the case of a terrorist attack occurring after a watchlist was finalised but during a deployment which led to the adding of any identified suspects of this to the watchlist. This still requires compliance with the relevant procedures and the approval of the authorising officer to add individuals to the watchlist in this instance.

(II) The other exception is in the case of a person becoming missing during the deployment who is risk assessed as high risk and the addition is with the consent of next of kin. This would be considered proportionate to help locate that individual to assist in preventing them from coming to serious harm, especially as a standard police tactic in this instance would be to complete a media release with the consent of next of kin, whereas this would be less intrusive. This would not require the approval of the authorising officer but would still require compliance with the relevant procedures.

b) The creation of any Watchlist is specific to the deployment of LFR and informed by the intelligence case for the deployment; this is to ensure the currency, relevancy, necessity and proportionality of the inclusion of each image, person or other details within the watchlist for template creation and potential matching to a live feed.

c) Images on a Watchlist will be copies of images that are already lawfully held by the Constabularies or their partners for other purposes. In assembling the watchlist, all reasonable steps will be taken to ensure that the image is a valid one of the specific person intended for inclusion on that given Watchlist.

d) Authorising Officers need (when authorising a watchlist) to expressly consider and approve any use of images that are sourced other than from a Law Enforcement or National Security body that holds that image either for a law enforcement purpose under part 3 of the DPA 2018 or is processing it under Part 4 of the DPA. This is because particular privacy considerations may attach to an image where it originates from outside of a law enforcement or national security context, in a way that differs to scenarios where source images are originally held for law enforcement or national security purposes. For example, if the source image comes from a third party in a commercial or private context where it was originally processed for a specific purpose that does not usually see routine data sharing with the police. Then greater analysis will need to be done to ensure that this further use of the image for LFR purposes will still be compliant. Even when the Constabularies can lawfully hold the images, the need for the Watchlist to be a proportionate policing response requires the Authorising Officer to undertake a careful assessment of an individual's privacy expectations (both as regards their specific context generally and as regards to the context of the specific source image) against the policing need to locate them using LFR. The Constabularies' Force Procedure outlines considerations for Authorising Officers at Section 3.5.

e) On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow LFR personnel to consider and manage the risk of poor-quality images generating inaccurate LFR Alerts. The LFR system automatically assesses each image against a number of different factors to ensure it is of sufficient quality to upload to the watchlist to ensure the risk of false positives is not increased. Examples may include (but are not set as or limited to) assessing the image to ensure a clearly detectable face and facial landmarks are visible, enforcing minimum resolution thresholds of the image (i.e. if below certain pixels it will be rejected), ensuring the head orientation and pose is sufficient to allow a match (i.e. is face on as an angled photo may be rejected) or assessing for obstructions to the face.

   Rejected photos may, in certain circumstances and in accordance with the relevant policies, be overridden and accepted to be added to the watchlist by the LFR operator. This would only happen in exceptional cases due to this increasing the risk of false positives and requires the approval of the Authorising Officer. An example of this may be in the immediate aftermath of a terrorist attack with outstanding suspects and an ongoing persistent threat. In those circumstances for example greater tolerance of images that don't meet the image quality threshold but relate to this specific overriding threat may be allowed for and be considered justified. If the threat and risk to the public is so high that the benefit of locating and arresting this suspect and protecting the public, outweighs the negative of increasing the risk of false positives due to lower image quality, they may exceptionally be added to the watchlist.

f) All copies of Watchlists are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment. The specific Biometric data on the watchlist, copies of the photos used on the watchlist, and the metadata attributed to the individual uploaded to the watchlist will all be deleted from the specific files and locations that were used for the operational deployment of the LFR. To the extent that such data is a duplicate of data held elsewhere for purposes other than the watchlist, that source data will at all times remain on the source systems it was originally drawn from (e.g. original photo, name, offence etc.) in line with current retention periods which apply to such data regardless of the deployment or not. But that original source data is disaggregated and will not be processed collectively or as a group in the way it was when copies were put onto and collated as the watchlist. The non-identifiable criteria that the watchlist was created on will remain in line with current retention periods (e.g. all persons wanted on court issued warrant for arrest during this period in this area etc), and this would allow the watchlist to be recreated if this was required. A final manual review of investigations to check for proportionality for inclusion on the watchlist may lead to some persons being removed from the watchlist in the last steps before deployment (but there is no possibility of any additions only removal at this stage). With the existing systems the watchlist as it appeared prior to that final manual review could at a later date be replicated if need be. If the manual review does not remove any individuals, then of course the actual watchlist will also be replicable. However, where individuals do get removed this means the exact watchlist used on the deployment would not be able to be replicated. That said the only difference will be that the deployed watchlist would be a smaller subset of the replicable pre-review watchlist.

g) Minimum technical standards are imposed to ensure that the cameras used in the LFR system are of sufficient quality for the LFR system's needs in order to minimise the potential for false positive matches as well as failures to identify matches that actually exist.

h) The LFR system is designed to assist the Constabularies' personnel locate people, it is not intended, nor will it ever be deployed to automatically locate people or automatically instigate coercive action to locate people by itself. The LFR system will always work to provide intelligence by flagging potential matches to at least one officer for a decision on any further action rather than autonomously taking a decision on any action after making a potential match.

i) LFR deployments and the materials that support LFR deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

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

- Where the LFR system does not generate an Alert, any biometric template data obtained from the live feed at the deployment is (after no match is found) immediately automatically deleted during the live operation of the deployment as soon as possible in relation to each piece of data. The templates from the live feed will therefore be created and deleted on a rolling basis during the deployment); and
- Watchlists and their associated biometric templates are deleted as soon as practicable, and in any case within 24 hours following the conclusion of the deployment, as covered above. The watchlist biometric templates of course need to be held throughout the period of deployment because they are the data that all the potential live feed candidates are compared against. So, whilst there is no need to retain live feed templates once no match is found, there is an ongoing need to retain the watchlist templates in order to consider whether others who appear in the live feed are a match to any watchlist individuals.
- Where the LFR system generates an Alert, all the biometric data used for the purposes of the LFR matching is deleted as soon as practicable and in any case within 24 hours following the conclusion of the deployment. Other personal data such as details of the match taking place, the subsequent activity after the match and the associated metadata attached to the watchlist image that was shared with the officer conducting any subsequent action, will be retained in line with the wider non-LFR policies (including retention).

4.34 CCTV footage generated from LFR deployments (the live feed that is the source for the sample biometric templates that are subject to processing against the biometric templates from the watchlist) is retained for 31 days for the purposes of crime investigation and complaint/conduct investigation. Reports of crimes and complaints may not be made immediately but could reasonably be expected to be reported within 31 days, and then deleted, except where retained for an ongoing legitimate policing purpose. For example, this information might form part of the material that has to be disclosed as part of a trial and so the data will continue to be retained and processed as long as it is necessary for the purpose of that

criminal proceeding. Another example would be if a complaint was made against a police officer or member of staff and so retained in accordance with the Constabularies' complaints / conduct investigation polices. The retention would be in line with the Constabularies' retention periods under the Review, Retention and Disposal of Crime and Non-Crime Related Information Schedule.

Deployment location privacy considerations

4.35 Many deployment locations will be identified as being necessary by the specific intelligence case supporting the prospects of locating persons at the particular identified site and/or how LFR plays a role within wider policing tactics. However, Authorising Officers must also consider the reasonable expectations of privacy the general public may have, both generally wherever the location is but also as regards the specific considerations that might arise at the unique location being considered for the LFR deployment. Even if the LFR deployment is in a public space, care must be taken to consider whether the angle of the live feed captures detail beyond that public space such as by viewing into windows of private homes or sensitive locations or over fences into private land.

4.36 Even where a deployment is such that only public space is within the field of vision of the cameras there is a need to take careful consideration as to the specific nature of that public space. Footage of a standard commercial high street presents very different considerations to that say of a street with a religious building, or a refuge, a sexual health clinic or other similar potentially sensitive location. Some places, and the people expected to be at those places (by their nature) attract greater privacy expectations than others. It will be necessary to scrutinise whether the precise location of the proposed deployment is suitable and appropriate or whether adjustments are needed to accommodate any specific extra concerns of this nature. For example, this might be where there is only a single entrance to a sensitive location that would fall within the area covered by the LFR system and so individuals may be prevented from accessing (or decide they are unable to access) that building because of the deployment. In such circumstances the Authorising Officer might conclude to slightly adjust the deployment location so that the relevant entrance is outside the scope of the LFR system (unless coverage of that entrance is essential to the purpose of the deployment and the interference this creates to individuals is outweighed by the wider public interests in the deployment).

4.37 Authorising Officers also need to consider what measures are appropriate to identify the use of LFR when it is deployed both generally as well as in the particular context and physical constraints of the location, particularly where expectations of privacy may be greater. This is important to establishing if the proposed use for LFR, and the deployment location itself is proportionate. Measures identifying to the public that LFR processing is taking place must be appropriate and effective at each deployment, and so tailoring may be necessary (such as for example by ensuring signage is lit as needed for deployments where there are low light levels).

4.38 Authorising Officers should also consider if a proposed deployment location attracts particular privacy concerns by reference to those expected to be at a particular location at the relevant time. This will include considerations as to signage and format, in some cases additional languages beyond English may be advisable or required. Similarly, some contexts may need identification to be more

than just in written form in order to be effective where it is likely that at least some of the individuals that will be subject to the LFR will not be adequately made aware of the deployment by written material alone (for example because of reasons of disability or otherwise). Timing should also be considered when assessing proportionality in the context of the location and the purpose of the deployment. A deployment during working hours for a purpose relating to late night alcohol related violence is unlikely to be proportionate, especially if the zone of recognition includes the entrance to a sexual health clinic for example. To be proportionate that deployment should be limited to timings that are outside the working hours of the clinic and relate to the periods most relevant to the purpose (i.e. after closing time).

4.39 **Example:**

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

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

- The importance of using LFR in that location to realise a legitimate aim supports LFR's use; as well as
- The lack of a viable, less intrusive alternative available for use in the circumstances; and
- Any further mitigations to reduce any impact to the wider public in so far as it is possible to do so.
- Having considered all of the above the Authorising Officer is satisfied that the level of interference on the public in that particular location by the particular context and timing of the LFR deployment is justified and necessary in light of the significant and specific purposes the LFR deployment seeks to serve.

4.41 **Example:**

If there was a necessity and proportionality case, based on intelligence, to deploy LFR in a residential suburban area to locate a group of burglary offenders, then we understand there may be a greater expectation of privacy in this area when compared to a non-residential area. To mitigate this, depending on the circumstances we may provide additional communication about the use of LFR, for example by leafleting local residents or posting on local neighbourhood social media groups as well as taking care to ensure that the parameters of the deployment are appropriate for the aim such as by ensuring the timing matches the timeframes when the suspects are most likely to be present such as the period when the burglary activity most often occurs rather than say other periods such as commuting rush hours or school pick up times when it is known the system is likely to be exposed to significant numbers of persons unnecessarily.

Authorising Officers: When taking a decision to deploy LFR, Authorising Officers should record the measures taken to ensure the use of LFR causes the least possible interference to the person(s) sought and others. This should include explicit reference to any particular privacy considerations that may be relevant to a deployment location and any mitigations in place to impact the level of interference of the LFR deployment. Authorising Officers should then continue to review deployments of LFR to ensure the use case remains appropriate and take action to ensure that those operating such deployments keep them updated as to any relevant changes of circumstances.

Wider Human Rights Act Considerations

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

Article 9

4.43 The clothing and other items people wear can be an act of thought, conscience and religion and in normal circumstances, the police do not have the legal power to require a person to remove clothing (including any headdress) simply because they are passing the LFR system. Additionally, the location where people may pass the LFR system may also engage Article 9, especially for example if the Zone of Recognition could potentially have a negative effect on people being able to access a religious building and practice their faith.

4.44 **Example**:

The use of LFR can assist the Constabularies to ensure public safety, including at a place of worship where the intelligence case has identified a compliant basis for the deployment (such as a threat to the public). A decision to place a LFR deployment outside a place of worship or in a way that substantially impedes access to a place of worship can engage Article 9. In this context, the public safety considerations need to be balanced against the need to use LFR at that location. If the public safety policing objectives could be achieved by deploying the LFR system elsewhere, it would not be necessary to deploy LFR at the proposed location. If the threat is such that it makes it necessary to site LFR near to a place

of worship, Authorising Officers also need to determine if the infringement on Article 9 rights can be sufficiently mitigated, or if not decide if the infringement is disproportionate to the likely benefits of using LFR. Considerations would typically include the impact on those seeking to access a place of worship, the likely impact on the same people without LFR (being potentially impacted by other policing measures or site closures) and the benefits to safety LFR can bring to the public in that area. As always it will be necessary to demonstrate that there was no viable alternative to achieve the same aim which posed less of an interference. Engaging with the members of the public whose rights are likely to be interfered with in this regard is likely to be key. In the context where there is a public safety threat necessitating an LFR deployment outside a place of worship, the impact of that deployment on individuals Article 9 rights may be mitigated by advance engagement with concerned individuals who attend that place of worship which for example may enable them to make alternate arrangements during the deployment allowing both the deployment and the continued religious practice to go ahead simultaneously.

Articles 10 and 11

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

4.46 **Example**:

The use of LFR can assist the Constabularies in policing an assembly or demonstration, particularly where there is an intelligence case supporting there being a risk to public safety. Specifically, LFR can support police officers by efficiently searching for perpetrators of violence in crowded locations where it might otherwise be difficult to locate them. In deciding the use of LFR is necessary and proportionate, regard should be had to an individual's Article 10 and 11 rights – noting there may be expectations of a degree of anonymity in a crowd and that individuals may choose to alter their means of demonstration as a result of the LFR deployment. Article 10 and 11 rights must be weighed against the need to use LFR as a policing measure that enables an assembly to take place that might otherwise be disrupted or prevented by the risk to public safety. In making this decision, consideration should be given to factors which could minimise the impact of LFR. These include limiting the use of LFR in time and scope to the minimum needed to ensure safety, such as by having a focus placed on ensuring the public understand the use of LFR is to help them safety undertake their assembly and particular emphasis on being as clear as possible to the individuals appearing within the zone of recognition just how limited the processing of their data is unless they match with a watchlist image, where there is a legitimate basis for more extended processing.

Operational Duties

4.47 The 'operational duty' was first outlined in the case of Osman v United Kingdom[14] and concerned a failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Case law also supports that the police are under an Osman style duty to investigate serious allegations in a timely and efficient manner in order to uphold an individual's Article 3 rights.

4.48 The Osman operational duty has particular relevance to LFR in two contexts

(I) Where the deployment of LFR is being used to give effect to that positive duty by seeking to locate those posing a threat to the public or themselves where a real and immediate risk to life is identified and LFR is thought to provide a necessary and appropriate response to such risk.

(II) Where the Osman operational duty will be engaged upon an Alert being generated in relation to a person who is being located because they pose a threat, meaning that the duty will require measures to be proactively put in place on a precautionary basis in case that person seeks to evade officers after an alert is generated or otherwise act in a way that poses a threat to others.

Article 14

4.49 This right requires that rights and freedoms must be protected and applied without discrimination. This is based on the principle that everyone, no matter who they are, should enjoy the same human rights and have equal access to them. Article 14 is not a stand-alone right – there is a need to show that discrimination has affected the enjoyment of one or more of the other human rights, not that the other rights have been actually breached. The use of LFR will for example be relevant in circumstances where demographic performance of the LFR algorithm varies to such an extent that people of a particular demographic were more or less likely to see a False Alert generated against them.

4.50 As a result, there are two main points to consider in relation to the LFR system

(I) Does the LFR system's demographic differential performance vary by a particular demographic such as it results in a person suffering a discriminatory effect, and

(II) If there is a difference in treatment, is this capable of an objective and reasonable justification or not.

4.51 Within this LFR legal mandate, specifically in Section 5.2, there is detail as to how the performance of the chosen LFR system has been considered to ensure that these effects are minimised. The Constabularies' LFR Equality Impact Assessment also details this further as to impact of different groups and mitigating actions taken to reduce adverse impact. The setting of who is included on the watchlist on set

[14] Osman V The United Kingdom [1999] 1 F.L.R. 193 (ECtHR) (23452/94 via hudoc.echr)

criteria which are not directly discriminatory (such as offence type and how long they have been outstanding) alongside policies that seek to minimise or prevent indirect discrimination seeks to ensure there is no discrimination at this stage. Officers will consider training they have had and in line with their regular policing duties and responsibilities, will ensure that their actions do not discriminate.

5. Equality Act 2010

5.1 The Equality Act 2010 provides a legal framework to protect the rights of individuals and advance equality of opportunity for all. The Equality Act 2010 prohibits discrimination (i.e. an unjustified difference in treatment on the basis of a protected characteristic). The prohibition of discrimination applies to both direct and indirect discrimination. As public authorities, the Constabularies must comply with section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty ("PSED").

5.2 The Constabularies are required to take measures to ensure that the use of LFR complies with the Equality Act 2010. Particular attention is needed in two respects: (a) the technical performance of the LFR system (and then, if performance varies by any particular demographic), and (b) the operational deployment of the LFR system:

The technical performance of the LFR system.

5.3 The Court of Appeal Bridges decision makes it clear that the PSED requires the Constabularies to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the LFR system and procedure used does not have an unacceptable bias on grounds of race or sex (or any other protected characteristic). To assist the public with understanding how the Constabularies meets its PSED duties, the Constabularies have published the LFR Equality Impact Assessment. The Constabularies have in particular considered the following:

- **Independent evaluations:** Several studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result, the Constabularies have paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) https://www.nist.gov/ who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used.

  Secondly an independent evaluation of the NEC NeoFace algorithm has been completed by the National Physical Laboratory - frt-equitability-study_mar2023.pdf. The study examined the equitability and performance of the technology, with a particular focus on ethnicity, age and gender. The evaluation began in late 2021 and included ongoing review throughout the study period. Findings were subject to external oversight and academic scrutiny.

- Having reviewed the findings of these independent evaluations the Constabularies are satisfied that not only do they indicate that the performance of the systems can be operated in a manner that is both compliant and fair but

that the learning from those studies has provided clear mitigations that ensure the systems are operated to perform in a way that optimises accuracy, compliance and fairness (e.g. by applying the knowledge developed about threshold settings). Furthermore, in light of the above the Constabularies are satisfied that the particular LFR system identified (NEC Neoface) and the particular procedure and controls that are proposed to be used are such that the deployments will not have an unacceptable bias on grounds of race or sex (or any other protected characteristic).

- **Ongoing assurance:** The Constabularies' LFR Documents provide for ongoing evaluation and a post-deployment review process. This reflects the ongoing nature of the PSED duty and also offers the Constabularies a chance to monitor for technical issues by reviewing all alerts, including any incorrect ones and monitoring for trends.

5.4 Currently there is no nationally agreed standard for LFR, and no nationally approved or mandatory testing is available. It is therefore up to individual police forces exactly how they ensure they do all they reasonably can to fulfil their public sector equality duty.

5.5 In addition to having ensured that independent bias testing of the relevant LFR system had taken place, and that the results of the testing are acceptable to the Forces in terms meeting the PSED, there are additional robust operational policy and procedures that have been developed and are applied to LFR use to ensure that the criteria for the deployment of LFR and the way it is used by officers helps the Constabularies further reinforce their compliance with the PSED. Lastly, the Constabularies are committed to evaluation of all LFR deployments and identifying any further work from this that could reinforce their compliance with PSED. The Constabularies will have regard to the outcome of any academic studies that may impact their compliance with PSED.

The operational performance of the LFR system.

5.6 The Constabularies' LFR Documents are also responsive to the Subject, System and Environmental Factors to ensure the LFR system is suitable for its intended use and operating correctly. Subject, System and Environmental Factors including aspects such as camera configuration, camera location, lighting conditions, the distance at which people will pass the LFR system and points relating to an individual's age and appearance have been considered carefully in the Constabularies' LFR Documents to ensure the efficiency of the LFR system and the Constabularies' compliance with its Equality Act 2010 duties

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

No engagement will occur with a member of the public unless at least one officer has reviewed an LFR system potential match and reached their own

opinion that there is a match between the member of the public and the Watchlist image.

5.8 This means the LFR system is not making any solely automated decision to engage with the public or take any other action. The LFR system essentially provides information it has collated but it is the officer that makes this decision of whether there is actually a match and what action should follow that determination - just as officers make similar decisions to Engage with members of the public every day (without the support of LFR). The system is merely providing source information for the Officer to decide on whether there is a match or not. This is analogous to a scenario where one officer believes a person who appears in front of them is a match to a wanted photo, and that first officer passes the photo to a second officer indicating the person in front of them and asks if the second officer also thinks there is a match. The officer is best placed to make this decision, drawing on their training and policing experience and aware of their legal duties and obligations.

5.9 Similarly, the officer is best placed to consider how specific subject-related, system-related and environmental factors may have influenced the LFR system in the particular circumstances and context where it generated an Alert and if such factors combine to mean an engagement with a member of the public is not appropriate in the circumstances. An example might be in a public high street deployment where an alert is generated for an individual who is known to have previously violently resisted arrest and attack bystanders. In circumstances where the alert is generated at a time where the zone of recognition is crowded with many young families and others the Officer may instead of authorising an immediate engagement seek to allow the suspect to leave the crowded area first. Similarly if a hit is generated at the end of an engagement when the light levels have dropped significantly an officer might consider a generated match to be a false positive given the officer takes into account the effect of light conditions producing a darker than usual image and so leading to a false positive match to a dark reference watchlist image which in the Officers view would not have occurred if the live image captured had been better lit.

> **Authorising Officers**: In order to ensure that the officer is best able to make an informed decision on any engagement, all officers who are part of an LFR deployment are to have been briefed on the operation of the LFR system. This includes being made aware of subject-related, system-related and environmental factors that can impact performance. LFR engagement officers should also have been given training relating to unconscious bias given their key role in the engagement decision making process.

5.10 In addition to considering subject-related, system-related and environmental factors, the Constabularies' personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of other crime fighting techniques, for example, 'stop and search'. In this respect, it is important that the use of LFR is driven from the need to meet a legitimate aim, such as the prevention of crime and disorder. The Equality Impact Assessment and, where relevant, the Community Impact Assessment informs the policing plan to support the deployment of LFR in a way that upholds the Constabularies' Public Sector Equality Duty. Compliance with the Equality Impact Assessment will then be

monitored and reviewed for the duration of each specific deployment as well as general overarching reviews taking place periodically.

6. Data Protection Act 2018

6.1 The Constabularies process personal data for LFR for law enforcement purposes 'based on law'; specifically, its legal powers identified in relation to the common law and statute as regards law enforcement activity (noting that such powers are also subject to governing legal frameworks such as those covered in the human rights and equality considerations outlined in this Legal Mandate and the policies put in place by the Constabularies' LFR Documents). The Appropriate Policy Document and other LFR Documents published by the Constabularies allows the public generally (but especially those persons who might pass through an LFR system) and those who may be placed on a Watchlist to understand the standards the Constabularies operate to, including setting out the authorisation process and requirements imposed on the deployment of LFR, details about where LFR may be used, and the considerations and constraints relevant as to who may be placed on an LFR Watchlist.

6.2 Where data is processed for law enforcement purposes, such as the purposes of preventing crime and disorder, Part 3 of the Data Protection Act 2018 (DPA) regulates the processing, including sensitive processing, whether processed on a computer, CCTV, via still images or any other media. Any recorded image or dataset which can identify a particular person is 'personal data'. The DPA therefore applies to the processing of data for LFR in a number of ways including both the processing of images and other data in order to help in locating those on a Watchlist but also in terms of processing biometric information of members of the public to confirm they are not on a Watchlist. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

"For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

Authorising Officers: Authorising Officers already need be satisfied of the necessity to use LFR to prevent crime and disorder in the context of the Human Rights Act 1998. Similarly, to satisfy Section 35(5) DPA, they need to be content that the LFR system's processing of biometric data is strictly necessary for one or more law enforcement purposes. The law enforcement purposes should be clearly identified and the way in which the strictly necessary standard has been met in each case explained. A watchlist for a single deployment could be focused on one particular issue and law enforcement purpose (e.g. locating a group of persons wanted following a previous public order incident). However, it is more likely that most deployments will serve multiple purposes and the watchlist will therefore be a composite reflecting that fact. A single watchlist might therefore contain a group of people wanted for arrest in relation to public order, others wanted for breach of bail (both Law Enforcement Part 3 purposes) as well as high risk missing persons (a non-Law Enforcement UK GDPR

purpose). Each group will likely serve different purposes and be selected on different criteria, for example different crime types, different risk gradings of missing persons or different categories of warrants. A single composite watchlist for a specific deployment may rely on multiple and different law enforcement and other purposes in the context of different individuals. However, there must be a strictly necessary basis in place for each instance of Law enforcement sensitive processing under Part 3 DPA 2018, or in relation to UK GDPR processing such as for missing persons compliance with the enhanced requirements of special category data). Authorising Officers should contact Legal Services if they consider a proposed deployment may have additional or unusual date protection points to consider, and especially as regards to the less common UK GDPR processing based watchlists.

6.3 'Strictly necessary' in this context means that the processing must be more than merely 'necessary'. It must be processing that is required in order to give effect to a purpose which cannot reasonably be achieved through any other less intrusive means. Additionally, any sensitive personal data collected via LFR must not be used in a manner that is contrary to the relevant identified purpose or in any way that does not meet the high bar of 'strict necessity'.

Alternative policing methods to prevent threats to public security:

6.4 LFR may be deployed to police a high profile well-attended public event. When considering alternatives, in this example, other measures such as non-LFR connected CCTV or human spotter teams may be considered. However, they will not always be a viable and less intrusive alternative in the circumstances. For example:

- Whilst CCTV can help ensure event safety, it lacks the ability to effectively proactively alert officers to the potential presence of individuals of interest to them for necessary purposes such as crime prevention, apprehension of wanted individuals or locating missing persons. It requires live monitoring and for the person monitoring to just coincidentally recognise someone they know to be wanted.
- It may not be practical to expect officers to recognise larger numbers of people of interest to the Police given the nature and scale of the event, the numbers of officers available to police the event and the flow rate and number of people passing the CCTV system or spotter teams. This is especially relevant where the importance of making such identifications supports the use of a more suitable alternative such as LFR. This may also be considered more proportionate, for example, should 200 persons wanted for disorder be considered as plausibly attending an event or incident, it would be more proportionate to use LFR to seek to identify these persons rather than sharing 200 faces with 100s of officers.
- Where LFR is thought to offer further important protection to the public as opposed to other policing methods. For example, this may apply where the law enforcement purposes for a deployment include wider public safety considerations. These may include the need to locate those wanted by the

courts. Such persons may attend such a high-profile event and, pose a risk to the public generally. Alternatively, where there is concern that persons might attend an event to cause disruption or carry out criminal acts the deployment of LFR system and signage may significantly contribute to the prevention of such crime and the protection of the public attending by having a deterrent effect convincing those persons intending to cause trouble to not attend given the presence of LFR because they no longer feel safe in being able to hide within a crowd.

6.5 When considering how a particular deployment meets the required 'strictly necessary' standard for law enforcement deployments and the enhanced requirements for Sensitive processing under the UK GDPR, the Authorising Officer should consider all relevant factors including:

- What other policing methods have been used / discounted when seeking to locate an individual(s) on the Watchlist or to provide a series of tailored security measures;
- The importance of achieving the relevant purpose and the prospects of achieving the relevant purpose through the deployment of LFR at the proposed location with the proposed Watchlist (for example, is the deployment intelligence-led or otherwise supported by information which confirms that LFR can be expected to get results in the circumstances and context being contemplated);
- The size and scale of the planned LFR deployment and associated Watchlist and the level of processing anticipated as a result of the LFR deployment (both as to those on the watchlist and especially of those individuals who will pass through the zone of recognition; *and*
- If the relevant purpose which underpins the use of LFR is strictly necessary[15] and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to all the general and deployment specific protections and safeguards implemented).

Authorising Officers: Authorising Officers need to be satisfied that the requirements of the relevant legal regime are met for each deployment and in relation to each entry on the relevant watchlist.

In the context of processing for law enforcement purposes such as the location of persons who are arrestable on sight the processing must satisfy at least one of the Schedule 8 conditions set out below and the processing must also comply with the six data protection principles.

For the less common UK GDPR processing scenarios such as the inclusion of vulnerable missing persons on a watchlist for safeguarding reasons the processing must meet the enhanced requirements for processing special

[15] Or in the case of UK GDPR processing meets the relevant equivalent requirements for processing special category data

category data and in particular meet one of the requirements in Article 9(2) such as the 9(2)© basis that it is necessary to protect the vital interests of the data subject or under 9(2)(g) it is necessary for reasons of substantial public interest, or in the case of member so the public passing through the recognition zone it is in line with 9(2)(e) of personal data manifestly made public by the data subject.. We advise that for any proposed UK GDPR processing Authorising Officers should liaise with Legal Services to ensure the different requirements of the UK GDPR are fully considered.

6.6 For Part 3 sensitive processing at least one of the Schedule 8 conditions of the DPA must be engaged:

- Necessary for the exercise of a function conferred by an enactment or rule of law – for reasons of substantial public interest;[16]
- Necessary for the administration of justice;[17]
- Necessary to protect the vital interests of the data subject or another individual;[18]
- Necessary for the safeguarding of children and of individuals at risk[19].
- Is processing of personal data which is manifestly made public by the data subject[20]

6.7 **Example**:

The use of LFR will assist the Constabularies in fighting knife crime in support of its common law policing powers. LFR could be deployed to identify wanted offenders who have failed to comply with court bail relating to such offences. Such processing of the offenders arguably meets both the condition of being necessary for the administration of justice as well as being necessary for the exercise of the functions conferred on the police under both statute and the common law.

Used in this way, LFR would assist in the "prevention, investigation, detection or prosecution of criminal offences".

LFR offers advantages over other potential policing methods such as a police officer using a picture or a physical description to scan a crowd and try and spot an offender where positive results would otherwise be less likely, and the risk of people being missed higher. Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context LFR's use may be seen as strictly necessary to support the investigation of knife crime, to enable the Constabularies to effectively respond to a pressing social need.

[16] At [1]
[17] At [2]
[18] At [3]
[19] At [4]
[20] At [5]

For similar reasons, the court in the *Bridges* cases accepted the substantial public interest in the police using LFR to discharge their common law policing duties

6.8 The Constabularies have also undertaken a number of steps as identified in the relevant Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the LFR system.

Data Protection Impact Assessment*:*

6.9 A DPIA has been conducted to support the use of LFR in order to provide an assessment of the impact of the envisaged processing operations on the protection of personal data, which has then been used to identify and minimise the data protection risks present. The Constabularies' LFR DPIA will be under constant review in light of each LFR deployment and more generally on a no less than an annual basis. Additionally Authorising Officers authorising the use of LFR always remain obliged to ensure that there is a DPIA in place which is sufficient for each deployment. Specifically, consideration should be given to:

- If the risks and controls in the existing DPIA remain current and sufficient for their specific planned use of LFR; and
- If the specific planned use for LFR in their proposed deployment poses any other risks which are capable of mitigation beyond those measures identified in the existing DPIA or are simply not covered in it.

Data Protection by Design:

6.10 A number of data protection controls have been designed into the LFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated data protection compliance into all aspects of LFR processing activities. Implementing the data protection principles in an effective manner and ensuring that the necessary related safeguards are integrated into the processing activities themselves. The designed-in measures identified at paragraph 4.11(c) of this document (and covered in detail in the DPIA), include measures to:

- Limit the amount of personal data collected (for example by ensuring the principle of data minimisation is routinely applied when compiling images for a watchlist and when considering the scope of the zone of recognition);
- Limit the extent of personal data processing (such as regards the policies and procedures in place in relation to the handling of instances where LFR suggests a match, but the failsafe human operator disagrees);
- Limit the period of personal data storage and the uses/purposes that data can be processed for (as especially considered in relation to the relevant retention schedule and rules).

6.11 The Constabularies' LFR Documents and other published supporting information explain how the Constabularies are assured that its LFR system operates with a high degree of statistical accuracy and in a way that does not lead to unjust results between demographics.

6.12 The LFR system, as part of the privacy by design approach adopted, features a number of physical and technical security measures including:

- A requirement that images are transferred onto the LFR system using a secure file transfer system. This transfer system uses identity-based AES 256-bit encryption using FIPS 140-2 approved cryptographic libraries. This transfer is completed via a separate computer system that sits between the internet and the laptop that the LFR software operates on.
- The LFR system operates as a fully closed system with password protection to access the application. The system is not able to be operated remotely. The LFR system is physically protected by officers always being present when in use as well as being chained to the desk and securely wiped following each deployment.
- Role based access controls with limited user permissions are implemented on the LFR system alongside full compliance with recording and documentary requirements such as ROPA and Logging.
- All connections are directed through HTTPS within a closed system.
- Penetrative testing has been completed of the system, and it has passed these tests.
- A full audit is maintained of all user initiated actions undertaken during the course of a deployment, and
- Technical issues with the LFR system are always dealt with by a cleared member of the technical staff who supports the deployment of the LFR system.

Appropriate Policy Document:

6.13 The Data Protection legislation requires that, when sensitive processing is carried out under Part 3 or where certain processing of special category data takes place under the UK GDPR, the controller must have an appropriate policy document (APD) in place. The Constabularies have a general APD and have further supplemented this with a LFR specific supplemental APD covering how it will handle sensitive processing in relation to LFR deployments. This document covers:

- The Constabularies procedures, safeguards and accountability principles for complying with the data protection principles in connection with sensitive processing, and
- Explanations of the Constabularies policies as regards retention and erasure of personal data as regards LFR processing.

Data Protection Officer:

6.14 The Constabularies have appointed a Data Protection Officer (DPO) in compliance with the data protection legislation who has been consulted in relation to LFR and has been involved in the production and reviewing of the Constabularies' LFR documents. The DPO is available to inform and advise the Chief Constables (as data controllers) and the Constabularies' personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

7. Protection of Freedoms Act 2012

7.1 The Protection of Freedoms Act 2012 (PoFA) has seen the introduction of a surveillance camera code issued by the Secretary of State (the Code) and the appointment of a Surveillance Camera Commissioner. Section 33(1) PoFA requires the Constabularies to have regard to the Code for the use of LFR. This includes having regard to the 12 guiding principles that system operators should adopt. The Code makes a number of specific points in relation to automated recognition technologies which the Constabularies have regard to as below:

Code	The Constabularies' Approach
Fair processing information to data subjects	The Constabularies make information about their processing publicly available to data subjects. It makes information relating to the LFR and data processing available via its website. The LFR deployments are publicly disclosed with supporting information
Appropriate retention and disposal systems	The necessary systems are addressed by the Constabularies' LFR Documents
Suitable technological and physical security measures	These measures have been addressed by design and are also covered in the Constabularies' LFR Documents
Cameras of sufficient quality to meet the intended purpose	This requirement is addressed by the design of the LFR system
Monitored by trained individuals	The LFR system will always flag possible matches to trained personnel for a decision on any further action. In this way, the LFR system works to assist the Constabularies' personnel to make identifications rather than acting as an autonomous machine-based process devoid of user input

8. Freedom of Information Act 2000

8.1 The Freedom of Information Act 2000 (FOIA) provides public access to information held by public authorities. It does this in two ways:

- Public authorities are obliged to publish certain information about their activities;
- Members of the public are entitled to request information from public authorities.

8.2 In recognition of its FOIA duties, the Constabularies make significant LFR information available via its website. This includes summary information relating to LFR deployments including:

- Watchlist size;
- Total number of Alerts;
- Positive action and incorrect identification numbers;
- Arrests and disposal numbers; and
- Estimates of the total number of faces seen as people passed the LFR system.

8.3 The Constabularies will also be responsive to FOIA requests. Legal Framework and Governance Overview

Summary of existing legislation and related governance regards policing's overt use of Live Facial Recognition Technology