

Protective marking:	Official until date of publication
Publication scheme Y/N:	No
Title:	RETROSPECTIVE FACIAL RECOGNITION: LEGAL MANDATE
Version:	V 1.0
Summary:	Outlines the legal basis for the MPS's use of Retrospective Facial Recognition technology.
Branch/ OCU:	MPS DLS
Review date:	24/08/2026

---

## MPS RETROSPECTIVE FACIAL RECOGNITION: LEGAL MANDATE

<b>1</b>	<b>Legal Mandate.....</b>	<b>1</b>
<b>2</b>	<b>Legal Basis – Use of imagery .....</b>	<b>2</b>
<b>3</b>	<b>Human Rights Act 1998 .....</b>	<b>7</b>
<b>4</b>	<b>Equality Act 2010.....</b>	<b>20</b>
<b>5</b>	<b>Data Protection Act 2018.....</b>	<b>22</b>
<b>6</b>	<b>Legal considerations regarding using RFR in relation to the deceased .....</b>	<b>25</b>
<b>7</b>	<b>Freedom of Information Act 2000.....</b>	<b>26</b>

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

---

### 1 Legal Mandate

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

<b>Level One: Legislation</b>	<b>Legal power to submit a Probe Image for RFR Searching</b>	<ul style="list-style-type: none"> <li>a) Police and Criminal Evidence Act 1984</li> <li>b) Specific legal powers which are context dependant to purpose for which the Probe Image has been obtained.</li> <li>c) Common Law</li> </ul>
	<b>Legal power to undertake a RFR search against an Image Reference Library</b>	<ul style="list-style-type: none"> <li>d) Police and Criminal Evidence Act 1984</li> <li>e) Specific legal powers which are context dependant to purpose for which the images in the Image Reference Library have been obtained.</li> <li>f) Common Law</li> </ul>
	<b>Regulating the use of RFR</b>	<ul style="list-style-type: none"> <li><u>Operational</u></li> <li>g) Human Rights Act 1998</li> </ul>

		h) Equality Act 2010 <u>Data Management</u> i) Data Protection Act 2018
	<b>Requests for information in relation to RFR</b>	j) Freedom of Information Act 2000
<b>Level Two: Code and Guidance</b>	<b>Regulating the use of RFR</b>	a) Code of Practice for the Identification of persons by Police Officers – PACE Code D b) Information Commissioner’s guidance
<b>Level Three: MPS RFR Documents</b>	<b>Regulating the use of RFR</b>	a) MPS RFR Policy Document b) MPS Training Documents c) MPS Data Processing Appropriate Policy Document d) Data Protection Impact Assessment e) Equality Impact Assessment

## 2 Legal Basis – Use of imagery

- 2.1 To undertake RFR searching against a Probe Image, the police need to lawfully hold the Probe Image and the images in the Image Reference Library. The lawfully obtained image(s) may or may not have been gained with the intention that at, at some future point, it would be used for RFR searching. It may also be that the police do not take the image but otherwise comes into possession of it because, for example, they lawfully seize a device with imagery on it or are otherwise given imagery by the public.
- 2.2 This MPS RFR Legal Mandate outlines key legal bases for obtaining and using images that are particularly relevant to the MPS’s use case for RFR. These are not exhaustive and:
- (a) practitioners may seek legal advice from the Directorate of Legal Services for advice where a further legal basis is proposed for the obtaining and use of a Probe Image for RFR Searching;
  - (b) when Image Reference Libraries are considered for use with RFR Searching, the MPS RFR Policy Document provides for an approval process which includes the need to identify a legal basis for the search against an Image Reference Library. Again. The Directorate of Legal Service is able to advise as required.
- 2.3 Key legal bases for obtaining and using images:
- (a) Police and Criminal Evidence Act 1984 (PACE): A key application for RFR searching will be in the context of imagery of those detained at a police station or who otherwise fall within the scope of Section 64A following a ‘relevant event’<sup>1</sup>. It is a means to allow the police to investigate who a person is, what other offences they may be wanted for and, whilst a person

<sup>1</sup> As such term is defined at Section 64A(1B) of PACE and summarised later in this legal mandate at 2.3(a)(i).

is detained, for a purpose related to the prevention and detection of crime and/or the investigation of an offence – including to ensure the safety and wellbeing of the person detained as well as police officers and staff responsible for their detention in order that investigations may progress safely and effectively. Section 64A of PACE is therefore a particularly relevant power for the taking and use of photographs:

- (i) **When can photographs be taken?** An officer may take a photograph in line with Section 64A of PACE. This applies to those detained at a police station. Section 64A of PACE also allows photographs to be taken of a person other than when detained at a police station following the occurrence of a ‘relevant event’ – such term as defined at paragraph 1B of Section 64A includes (i) when a person is under arrest but not detained at a police station, (ii) when a person has been taken into custody by a constable after being arrested for an offence after being arrested for an offence by a person other than a constable, (iii) a person who has been made subject to a requirement to wait by a community support officer under paragraph 7 of Schedule 3B to the Police Reform Act 2002 (iv) a person given a direction by a constable under Section 35 of the Anti-social Behaviour, Crime and Policing Act 2014 and (v) a person who has been issued with a penalty notice for disorder or a financial penalty notice.
  
- (ii) **Is consent needed?** Section 64A (1A) allows the taking and use of the photograph to occur with appropriate consent or, if appropriate consent is withheld or is not practicable to obtain it, without it. PACE CODE D provides some non-exhaustive examples of when consent may not be practicable including:
  - (A) if a persons is drunk or otherwise unfit to give consent;
  - (B) where there are reasonable grounds to suspect that if a person became aware that a photograph was to be taken, they would take steps to prevent it being taken (for example through violence or other resistance such as covering their face) or that it would otherwise not be possible to take it;
  - (C) in the case of a juvenile, if a parent or guardian cannot be contacted in sufficient time to allow the photograph to be taken; and
  - (D) on occasion where it is necessary to take the photo covertly – on these occasions there should be a clear rationale as to why the necessity case arises and what means it is more than merely desirable to take a covert image.
  
- (iii) **What can the image be used for?** Section 64A(4)(a) provides that an image taken under the power can be:
  - (A) used by, or disclosed to, any individual for *any purpose related* to the prevention or detection of crime, the investigation of offences or the conduct of prosecutions by, or on behalf of, police or other law

enforcement and prosecuting authorities inside and outside the UK or the enforcement of a sentence; and

(B) after being so used or disclosed, may be retained but may not be used or disclosed except for a purpose so related (together, the **64A Purpose Limitation**).

(iv) The nature of the *any purpose related* statutory power, provides a legal basis to submit an image taken under Section 64A PACE for RFR searching providing such action would be in accordance with the wider legal framework that regulates the use of RFR (notably human rights and data protection considerations) .

(v) PACE Code D provides some examples of what would fall within the 64A Purpose Limitation. This helps support a number of use cases the MPS has for RFR which include:

RFR Use Case	PACE Code D Power (Note 5B)
Checking if a person is sought for other offences	<i>“checking the photograph against other photographs held in records or in connection with, or as a result of, an investigation of an offence to establish whether the person is liable to arrest for other offences”</i>
Seeking to verify a person’s real identity	<i>“when the real identity of the person is not known and cannot be readily ascertained or there are reasonable grounds for doubting a name and other personal details given by the person, are their real name and personal details”</i>
Confirming a response to bail	<i>“when a person has answered to bail at a police station and there are reasonable grounds for doubting they are the person who was previously granted bail, using the photograph to help establish or verify their identity”</i>
Confirming the execution of a warrant	<i>“when the person arrested on a warrant claims to be a different person from the person named on the warrant and a photograph would help confirm or disprove their claim”</i>

(b) Other case-specific statutory powers which enable the taking of an image for RFR Searching:  
 The MPS also has other statutory powers that, where applicable, provide the power to take photographs and would include their use within an RFR system in order to seek matches against other imagery. These include:

(i) **The Terrorism Act 2000 (TACT):** A person may be detained under Section 41 TACT or examined under Schedule 7 of TACT for the purposes of determining a person if a person is, or has been, involved in the commission, preparation of instigation of acts of terrorism. Paragraph 2(1) of Schedule 8 to TACT empowers an authorised person to take any steps which are reasonably necessary for photographing a detainee, measuring them or identifying them.

(ii) **The Counter Terrorism Border Security Act 2019 (CTBSA):** Similar powers to Schedule 7 TACT exist under Paragraph 26(1) to Schedule 3 of CTBSA where

an examination may occur for the purpose of determining whether a person is, or has been, engaged in hostile activity with a corresponding power to take photographs arising. In light of the power to use the photographs for the purposes of identifying a detainee or a person subject to examination, and pursuant to the applicable Codes of Practice, an ability to use the photograph to verify that a person is not a particular person, there is a legal power to undertake RFR searching for images obtained following an examination under Schedule 7 TACT and/or Schedule 3 CTBSA (as applicable).

- (iii) **Immigration Powers** – Paragraph 18 to Schedule 2 of the Immigration Act 1971 provides a power for a constable to take such steps as may be reasonably necessary for photographing, measuring or otherwise identifying a detained person and accordingly provides policing with a power to take photographs and submit them for RFR Searching when seeking to identify them.

**Key point:** The above statutory powers are non-exhaustive but provide examples of how specific areas of policing benefit from further statutory powers to take *and* use photographs of people's faces for RFR Searching. Whilst the above narrative does not necessarily confirm any such use of the powers will occur, it also shows how, in specific cases, statute imposes a duty on a person to allow their photograph to be taken by the police. Importantly, the common law (discussed below) provides general powers for the police to take photographs of people. It does not impose a legal duty on a person to have their photograph taken and/or make their face available for photographing by the police.

- (c) Powers to bring photographs into policing possession: Not all photographs used by policing to undertake RFR searching will have been taken by the police. They may instead be given to the police or otherwise brought into policing possession and then benefit from powers granted to policing to analyse such data. This may occur for example when:
  - (i) police benefit from the voluntary provision of a device with the agreement to extract information in line with Chapter 3 of Part 2 of the Police, Crime, Sentencing and Courts Act 2022 and its associated Code of Practice.
  - (ii) police exercise powers of seizure or retention (the exact powers being used will be context dependent with common recourse being made to power of seizure under the Police and Criminal Evidence Act 1984).

Further analysis of policing powers to bring items lawfully into policing possession is beyond the scope of this RFR legal mandate (as it relates to wider powers used in policing investigations generally) other than to note that any use of such image as a Probe Image for RFR searching must be first predicated on the image being lawfully in police possession.

- (d) Common law powers: In the absence of a specific statutory power, the MPS may rely on its common law powers to take photographs more generally and use them for submitting a Probe Image to RFR technology for searching. Key policing common law powers include those:
  - (i) protect life and property;
  - (ii) preserve order and prevent threats to public security;

- (iii) prevent and detect crime;
- (iv) bring offenders to justice; *and*
- (v) uphold national security.

**Example:** The MPS may use RFR to seek to help locate missing persons in order to protect life in line with its safeguarding responsibilities at common law. In these circumstances, a family member may provide the MPS with a photograph of a missing person. Running a RFR Search using this Probe Image would not benefit from a specific statutory power to support the use of the Probe Image. However the results of such a search could be critical to the police and ensuring that person's safe location. By way of example, it may allow policing to piece together the missing person's movements from footage and other imagery to determine who they have recently been seen with. In these circumstances, the common law would provide the MPS with the legal basis to use the Probe Image for RFR Searching.

- (e) In relation to the use of common law to support the taking of photographs and using a Probe Image to undertake an RFR Search:
  - (i) The courts have recognised that “the rules need not be statutory, providing they operate within a framework of law and that there are effective means of enforcing them”.<sup>2</sup>
  - (ii) **Policing powers to take photographs at common law:** In *R (Wood) v Commission of Police of the Metropolis* [2010] 1 WLR 123, the police took and retained photographs of the claimant in the street for the purpose of gathering evidence about possible disorder and criminal conduct. There, Laws LJ and Lord Collins held that this was lawful (see [50] – [55] and [98] – [100]). As Lord Collins observed at [98], “*The taking of photographs in the present case was lawful at common law, and there is nothing to prevent their retention*”. This was supported by the Court of Appeal in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058 which noted “Just as the human eye can observe a person in a public place, so the police have the power to take photographs of people”.
  - (iii) In the case of *R (Catt) v Chief Police Officers* [2015] A.C. 1065, Lord Sumption recognised that applicants could have their personal information noted down and retained by the police as they occupied publically accessible space. The court recognised the police's common law powers to collect and store information are subject to an “intensive regime of statutory and administrative regulation” under the Data Protection Act and various guidance documents on the management of police information.
  - (iv) **Policing powers to use photographs at common law:** The courts have further recognised the right of the police to make use of a photograph of an individual. The courts accepted the purposes of preventing and detecting crime, the investigation of alleged offences and the apprehension of suspects or persons

---

<sup>2</sup> *R (Catt) v Association of Chief Police Officers* [2015] A.C. 1065 at [11].

unlawfully at large. This was the case whether or not the photograph is of any person they seek to arrest or of a suspect's accomplice or of anyone else. The court confirmed the "key is that they must have these and only these purposes in mind and must ... make no more than reasonable use of the picture in seeking to accomplish them".<sup>3</sup>

- (f) In a different application, the use of the police's common law powers and PACE as a legal basis to support facial searching has been considered and recognised by the courts in the context of Live Facial Recognition in:
- (i) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin); and (on appeal in)
  - (ii) *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
- (g) Whilst the composition of a Watchlist (for a Live Facial Recognition deployment) is different to submitting a Probe Image for retrospective searching, not least because one seeks to locate a person(s) in a public space in real time and the other is seeking a person by searching against existing imagery records, in many cases, the wider policing purpose for the use of facial recognition technology will be the same – the prevention and detection of crime and/or ensuring public safety. In this purposive context, it is valuable to note that the Court of Appeal recognised that legal basis for the compilation of Watchlists in a live context could be "both authorised under the Police and Criminal Evidence Act 1984 and within the powers of police at common law."

**Key point:** Where officers are considering conducting an RFR Search using a Probe Image obtained in reliance of a legal power not covered in this legal mandate, legal advice should be obtained from the Directorate of Legal Services.

**Key point:** Prior to approving an Image Reference Library for RFR searching, its legal basis and its ability to be used for RFR needs to be established and recorded.

### 3 Human Rights Act 1998

- 3.1 All MPS use of RFR will be in compliance with the Human Rights Act 1998. RFR technology engages the Human Rights Act 1998 and in particular has the potential to impact upon an individual's Article 8 rights, the right to respect for private and family life. This provides:

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

---

<sup>3</sup> Per Laws J in *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 at 810F

3.2 In relation to a Probe Image: A photograph of a person, where it is of a standard to use it as a Probe Image, represents that person's personal data. From it, that person could be recognised and its taking and retention has been accepted to amount to an interference with Article 8.<sup>4</sup> The use of RFR to search against an Image Reference Library is also an act of interference with Article 8. The overall act of running a RFR Search:

- (a) involves the creation of a biometric template of the person's facial features – this requires specific technical processing which is for the purpose of uniquely identifying an individual. This template comprises biometric data for the purposes of Section 205(1) of the Data Protection Act 2018<sup>5</sup>. A greater level of sensitivity attaches to this type of data and this was recognised by the Court of Appeal in the context of LFR in the *Bridges* case<sup>6</sup>; and
- (b) aims to find matches against the Probe Image from within an Image Reference Library. Such matches can be revelatory and provide intelligence leads for further investigative activity. Depending on the level of detail held by the police in relation to an individual, a match may help the police identify that person and/or link a person to previously frequented locations, their associates, and information held by the police about their policing record or their pattern of life.

3.3 In relation to an Image Reference Library: Images of persons held on a dataset by policing comprise personal data. *Gaughran v United Kingdom* recognises that there is a sensitivity to a dataset over a disaggregated collection of images noting:<sup>7</sup>

*“The building up of a database of such data from those convicted of offences provides a very useful and proven resource in the battle against crime by reason of the assistance it provides in identifying individuals. It is clear that the larger the database the greater the assistance it will provide. While a universal database would be of immense help in combatting crime, weighing the private rights of individuals against the good which would be achieved by such a universal system requires the striking of a fair balance. Experience has shown that those who have committed offences may go on to commit other offences. A state decision to draw the line at those convicted of a substantial category of offences is entirely rational and furthers the legitimate aim of countering crime so as to protect the lives and rights of others.”*

3.4 The effect of *Gaughran* is to mean that, compared to an image in isolation, an image enrolled into an Image Reference Library and made available for RFR Searching can potentially say more (about the person in the image) to more people (i.e. the RFR Search users of the Image Reference Library). For this reason Article 8 is engaged by the retention and RFR Searching of an Image Reference Library. This now extends to custody images as, in *Gaughran*, the court recognised for the first time that that the taking and retention of custody images amounts to an interference with Article 8.

---

<sup>4</sup> See for example, para 64 of *Gaughran v United Kingdom* (13 February 2020, Application 42345/15)

<sup>5</sup> [Add link to DPA section]

<sup>6</sup> See para 88 of the judgment.

<sup>7</sup> At para 44 of the judgment.



3.5 The degree of interference: The courts have considered the intrusion resulting from biometrically templating a person and using that template to undertake facial recognition comparisons against a list of persons sought by the police. They did so in *Bridges* in the context of LFR and those passing the system who did not generate an Alert. There, the Court of Appeal accepted that whilst Article 8 was engaged in relation to those passing an LFR system, there was a “negligible” impact on a person’s Article 8 rights. A similar position applies to RFR, *until a point where a potential match is returned*. This is because:

- (a) both actions (passing the LFR system and running an RFR Search) involve the creation of biometric templates;
- (b) both passer-by and Probe Image biometric templates are deleted after the FR search is run unless a potential match is returned or the image requires further searching by way of the Unresolved Crime Cache;
- (c) both are not revelatory to policing unless and until a potential match is returned – other than providing a negative assurance that a person is not on a LFR Watchlist / Image Reference Library (as applicable).

3.6 Nevertheless, at the point where the RFR system does return a result, then there is a greater interference with Article 8 which moves beyond the ‘negligible’. This is because there is a greater intensity of data processing, a greater scrutiny of that individual (including cross-referencing to other data to validate a Potential RFR Match), a revelatory effect given a potential link to other data will have been made by the RFR System and greater potential consequences to that person should the match be viable. This can be anticipated when seeking to undertake an RFR Search and therefore the nature of the intrusion needs to be considered holistically, and capable of justification prior to the RFR Search against a particular subject being undertaken.

**Key point:** The legitimate aim driving the RFR Search needs to be sufficiently important to make out the necessity and proportionality of undertaking an RFR Search (including any policing tactics required during the Adjudication process which may need to follow a Potential RFR Match). An assessment of the expectations of privacy that attach to (i) a Probe Image and (ii) an Image Reference Library is needed as part of this overall assessment.

The MPS RFR Policy Document provides a structure to help do this by the way of tiered Image Matrix (Annex) with associated approval requirements. These tiers reflect the differing sensitivities attaching to images be they provided/taken:

- (a) in compliant or non-compliant circumstances.
- (b) in overt or covert circumstances;
- (c) by law enforcement or shared to law enforcement;
- (d) at a location or in other circumstances which raise elevated privacy considerations.

3.7 Justifying an interference with Article 8: As a qualified right, any interference with an individual’s Article 8 rights is only permissible if:

- (a) there is a legal basis for the interference with the qualified right that the public can understand;
- (b) the use of RFR seeks to achieve a legitimate aim;
- (c) it is necessary for the purposes of that aim in a democratic society; *and*
- (d) the use of RFR is proportionate to the legitimate aim being sought.

3.8 It is well-established that the reach of Article 8 can be broad. The case of *S v. United Kingdom*<sup>8</sup> confirms that this can relate to a person's right to their biometric data and any storing of data relating to it. Recognising that RFR involves biometric processing, that case went on to recognise that, in protecting the personal data and other forms of biometric processing, the interests of the data subject and the community as a whole "may be outweighed by the legitimate interest in the prevention of crime".<sup>9</sup>

3.9 There is a legal basis for the interference with the qualified right that the public can understand.

3.10 In *Glukhin v Russia*<sup>10</sup> citing *S. and Marper v. the United Kingdom*<sup>11</sup> the European Court of Human Rights states:

*"it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."*

3.11 In the *Glukhin* case the court had 'strong doubts' that the Russian legal system met the 'quality of law test' – noting that Russian domestic legal system did not contain "any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or on the processing of personal data." In the case of the MPS's use of RFR, the RFR Legal Framework (outlined at paragraph 1.1) provides the legal basis for interference with an individual's Article 8 rights and regulates the use of RFR Searches. It contains safeguards which enable the necessity and proportionality of the interference with Article 8 rights (and the processing of personal data) to be anticipated and examined. It ultimately provides a framework by which individuals can hold the MPS to account and to seek redress.

3.12 In considering if the use of RFR is compatible with the rule of law, there is a need to consider the twin requirements of accessibility and foreseeability.

(a) To be accessible to the person concerned, the legal basis needs to be published and comprehensible. It must be possible to discover what its provisions are.<sup>12</sup>

(b) To be foreseeable it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than the law itself'.<sup>13</sup> The requirement for what can be termed

---

<sup>8</sup> (2009) 48 EHRR 50, at [66 and 67]

<sup>9</sup> At [104]

<sup>10</sup> No 11519/20 at [77]

<sup>11</sup> No 20562/04

<sup>12</sup> *Sunday Times v United Kingdom* (1979) 2 EHRR 245, *Silver v United Kingdom* (1983) 5 EHRR 347, and *Malone v United Kingdom* (1984) 7 EHRR 14.

<sup>13</sup> *Per Lord Sumption* [17] in *Re Gallagher* [2019] 2 WLR 509

'reasonable predictability' does not mean that the law has to codify answers to every possible issue.<sup>14</sup>

3.13 Accessibility: The RFR Legal Framework which underpins the MPS's RFR capability benefits from a number of steps to ensure it is sufficiently accessible to meet the quality of law test. In particular the RFR Legal Framework benefits from primary legislation for its use of custody images and a number of other case-specific use-cases identified in this legal mandate, published and often-cited case law, and published Codes of Practice (including in relation to PACE, Border Powers, TACT and the voluntary provision of a device with the agreement to extract information).

3.14 In relation to use-cases for RFR Searching, particularly where the legal basis is the common law, the Court of Appeal in *Bridges* recognised that published policy documents can also enable a police force to comply with the quality of law requirement.<sup>15</sup> Recognising that in this particular instance, certain matters such as when an RFR Search may be undertaken require policy in order to meet the quality of law test, specifically around foreseeability, the MPS has published its RFR Documents.

3.15 Foreseeability: The use of RFR should be undertaken in a way that is predictable. It does not require "an over-rigid regime which does not contain the flexibility which is needed to avoid unjustified interference with a fundamental right" but does mean "safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate interference with Convention rights".<sup>16</sup>

3.16 In *Bridges*, in the context of live facial recognition, the court recognised two questions arose that conferred too greater a discretion on officers to determine policy on a case-by-case basis such that the overall use of live facial recognition in that specific case was found not to be foreseeable and therefore in accordance with law. These two questions were termed by the Court of Appeal to be the 'Who Question' and the 'Where Question' – in essence who could be placed on a LFR Watchlist for location and where LFR could be deployed to locate the people on an LFR Watchlist. A similar position exists for RFR especially when drawing on common law powers and the questions for the MPS are addressed by way of a published policy. This provides an answer such that the use of RFR by the MPS for its use-cases can be foreseen by the public. These points may be termed the 'What Question' and the 'How Question' and essentially go to the points where RFR results in interference with Article 8 Rights and involves sensitive data processing.

(a) The 'What Question' – this is a question as to the images which may be used for RFR Searching and what controls, safeguards and approvals attach to them? The MPS RFR Documents answer this by:

- (i) placing controls and safeguards around the selection and use of Probe Images for RFR Searching including the adoption of a tiered approach to the selection of Probe Images that focuses consideration on the sources of Probe Images and the expectations of privacy that attach to such images;
- (ii) outlining the process by which approved Image Reference Libraries may be searched. The controls and safeguards are designed to recognise that

---

<sup>14</sup> Per Lord Sumption in *Catt* at [11].

<sup>15</sup> See for example [94].

<sup>16</sup> Per Lord Hughes in *Beghal v Director of Public Prosecutions* [2016] AC 88 at [31] and [32].

different Image Reference Libraries have differing level of sensitivity and it is necessary to ensure undue data processing is minimised when a less intrusive Image Reference Library would allow the policing objective to be achieved. Accordingly the MPS RFR Documents implement a staged process to RFR Searching outlining an approval process to approve an Image Reference Library as being eligible for RFR Searching both in relation to Substantive Image Reference Libraries with ongoing utility to the MPS and Ad Hoc Image Reference Libraries of relevant to a specific investigation or operation;

- (iii) implementing specific controls and safeguards in relation to certain protected characteristics – including where a risk of exploitation may otherwise arise;
- (iv) providing direction to both those being asked to approve the use of an Image Reference Library for RFR Searching and those undertaking RFR Searching in terms of how Image Reference Libraries may be approached in terms of the intrusion and data processing that attaches to them and when elevated privacy considerations may arise; and
- (v) detailing when images may be selected for ongoing RFR Searching against holdings against the MPS' Image Reference Libraries and the further controls and safeguards which attach to this process.

(b) The 'How Question' – this is a question as to how an RFR Search should be undertaken including how officer decision making is channelled to ensure safeguards are in place to undertake a proportionate search, targeted on need as opposed to facilitating a 'search all' approach or allowing undue levels of discretion. The MPS RFR Documents answer this by:

- (i) outlining the purpose and specific grounds for when an RFR Search may be undertaken – this approach limits undue discretion and ensures that searches have a policing objective;
- (ii) detailing the pre-requisites to undertake an RFR Search to ensure less intrusive options have been considered and that a necessity case to act is made out;
- (iii) specifying the process to undertake an RFR Search and the approvals that attach to RFR Searching; and
- (iv) detailing the role of the human-in-the-loop during the Adjudication process and ensuring the nature of RFR Search results are disseminated as part of any results.

### 3.17 The use of RFR seeks to achieve a legitimate aim.

Article 8 recognises action in the interests of national security, public safety and the prevention of disorder or crime as legitimate aims. The use of RFR in line with the MPS RFR Documents will help the MPS to achieve its law enforcement purposes.

**Key point for RFR Users:** At the point that it is decided to undertake an RFR Search, the user should be clear as to its purpose and how using RFR will help the MPS realise a legitimate aim. Within the MPS, permissible purposes and grounds for RFR Searching are defined in the MPS RFR Policy.

### 3.18 The use of RFR is necessary for the purposes of that legitimate aim in a democratic society

RFR will be used in response to a pressing social need by helping the MPS to deliver on its policing responsibilities. It enables the MPS analyse the imagery it holds to help the MPS undertake investigations in an efficient and effective way compared to lengthy manual alternatives. It reflects the need to use of proven technologies to better equip officers to tackle criminality and focus their time to greatest crime-fighting effect. It is therefore a tool that helps the MPS to discharge its operational, investigative and safeguarding policing responsibilities.

**Key point for RFR Users:** When considering undertaking an RFR search, the RFR User needs to be mindful that Article 8 is engaged by that search. Accordingly, the policing need that underpins the purpose for the search must be sufficiently important to justify it such that the search is necessary - both in terms of (i) the use of the Probe Images and (ii) the Image Reference Libraries against which the RFR Search is conducted. Necessity in this context should lie somewhere between 'indispensable' and something which is more than merely 'desirable'. RFR Users need to keep a record why they considered undertaking an RFR Search to be necessary, including the problem the search was seeking to address (i.e. the search purpose), what has been done to date and ensure that other less intrusive options have been considered prior to turning to RFR.

The following are examples of why RFR may be used as a necessary tool to assist the MPS in discharge of its law enforcement purposes. The examples are illustrative only should not be taken to infer limits on the circumstances in which RFR can be lawfully be used:

**Terrorism:** The use of RFR will assist the MPS in fighting terrorism. By way of example, in the immediate aftermath of a terrorist attack, there is often a large volume of imagery (including video excerpts) that need to be analysed at pace to identify those responsible, to establish their movements, assess the likelihood of further atrocities and progress a criminal investigation at pace. Facial imagery is often important and, in an era of a digitised society where people have camera phones, it is usually a lead available early to investigators in such investigations. Whilst this presents its own challenges in terms of the volume of footage and imagery, in such circumstances RFR may be used to help more swiftly analyse footage and imagery against Image Reference Libraries to determine if subjects of interest were present in the events surrounding the atrocity. Using RFR in this way, offers the MPS a focused and rapid capability to help the MPS achieve its aim of preventing and detecting crime and disorder and protecting the public through the investigation and disruption of those seeking to commit terrorist offences.

**Mitigating the ongoing risks in detention and enabling the effective investigation of**

**crimes:** When a person is detained at a police station, it is important that the police are able to:

- effectively and efficiently identify a person in detention;
- understand the totality of any involvement that the subject may have with criminality given the public interest in delivering an effective criminal investigation;
- assess the risks they pose to the public, themselves and officers whilst facilitating their detention in order to be able to progress their investigations efficiently and safely in a way which best delivers the MPS' law enforcement objectives.

It is in this context that decisions are made about how an individual's detention is managed, the level of care they need, and protective measures officers may need to take where a risk of harm to them is identified. Individuals may not always be able or willing to highlight their needs or flag the risks they pose to others. RFR offers an important capability alongside other biometric modalities (given not all modalities may be held by policing) in regular use in the custody environment to link a person to the policing information held about them such as violence or ailment markers.

It is also important in the context of using RFR to ensure that the policing investigation that brings the person to the police station is fully investigated and that links to other offences are also explored. RFR provides an important capability in this respect, it allows faces to be linked across a variety of images (be it relating to the same offence or difference offences). It therefore allows criminal investigations to be accelerated in a way that a manual or less precise search of imagery would not facilitate. This minimises the time needed in detention which would be elongated by less capable processes, enables a prompt and effective investigation to be undertaken and also allows the risk to the public to be fully considered.

**Crime:** The use of RFR will assist the MPS in discharging its duties to deliver prompt and effective criminal investigations. By way of example, in the context of complex criminal investigations, it is often necessary to establish the movements of persons within imagery and short video provided to the MPS by the public following an appeal. This can involve painstaking manual analysis of imagery and video clips at a time where the need for prompt analysis is critical to the progress of an investigation. RFR offers investigating officers an effective and efficient opportunity to seek to retrospectively understand where a subject appears within media and their movements around the time of a crime. This is particularly helpful should a person be seeking to change their clothing and appearance that may otherwise frustrate more manual processes. Using RFR in this way, offers the MPS a focused and rapid capability to help the MPS progress its investigation. Undertaking a prompt and effective investigation attracts a significant public interest in the context of effecting faster arrests and the management of the risk to the public. It also increases the prospects the effective administration of justice not least because timeliness can often prove critical in securing evidence to enable successful prosecutions.

**3.19 The use of RFR is *proportionate* to the legitimate aim being sought**

When considering the use of RFR, the benefits of using RFR for an investigation or operation should not be disproportionate or arbitrary.

In this respect, the following factors (amongst others, depending on the nature of the Deployment) will guide those requesting and giving approvals in relation to RFR:

- (a) *The use of RFR should be a reasonable use of MPS powers - it will not be proportionate if the proposed use of RFR is excessive in the overall circumstances of the investigation, operation or other policing activity.*

This requires consideration of the legitimate policing purpose and the potential benefits of using RFR in order to progress it. This needs to be balanced against the interference caused by undertaking a RFR Search using a Probe Image against an Image Reference Library. In this context the following points are particularly relevant when reaching a judgment as to proportionality:

1. The MPS has defined RFR Search Purposes and RFR Search Grounds which need to apply to ensure there is a policing basis and law enforcement need for undertaking an RFR Search.
2. The MPS RFR Policy Document advocates a staged approach to searching against Image Reference Libraries to ensure the intrusion on people's expectations of privacy are minimised to that which is necessary.
3. In relation to Probe Images, the MPS RFR Policy Document requires consideration be given to ensure the relevance of Probe Image(s) proposed for Searching.
4. The MPS RFR Policy Document provides a 'Levels' approach to Probe Images to ensure their intrusiveness is considered with higher levels being subject to further approvals to ensure that the act of using the Probe Image is not disproportionate to the policing need.
5. The MPS RFR Policy Document reflects the need to consider the RFR process as a whole. The approach requires the whole process to be considered, in terms of what may be reasonably anticipated to ensure that RFR Search results would be actionable and the process as a whole not unduly excessive before committing to it.

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

**Key point:** The use of RFR should be considered against other investigatory methods. 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 operation.

The MPS RFR Policy provides for a requirement to have regard to relevant Pre-RFR Checks to ensure other less-intrusive options have been undertaken or otherwise considered and (i) dismissed as not viable or (ii) pursued in tandem with an RFR Search where the urgency of the need does not support awaiting the result of the Pre-RFR Checks.

It is also notable that an RFR Search may offer a less intrusive option compared to other policing tactics – for example a public appeal for a missing subject where that communication is likely to create an enduring online presence. A facial biometric is also less sensitive biometric than some other biometric modalities. The principle that differing biometrics have

differing sensitivities is recognised in *S v United Kingdom*<sup>17</sup> where the Court recognised that fingerprints are a source of significantly less personal data than a DNA sample. As such facial recognition may be a more proportionate, less intrusive solution available to officers than other alternatives. This is because facial biometrics are not universal but linked to a proprietary facial recognition system such that they are also not as revelatory or come with the same exploitation risks in terms of health matters unlike DNA.

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

RFR will be used for a limited time, with limited grounds for defined policing purposes. The Probe Images for searching are selected based on their relevance to the policing need and unless a potential match occurs during the RFR Search process, the collateral intrusion is limited both in terms of the ability to select faces (in images of multiple faces) and numbers of results.

**Proportionality controls – ‘designed in’.** Controls are also designed in to the RFR system and its operation to help minimise any impact on those in a Probe Image and/or an Image Reference Library as follows:

1. Probe Images:

- a. **Selection:** a human decision is needed to select Probe Images for RFR Searching – there is no automatic decision to submit for RFR Searching. This ensures the use of RFR is focused.
- b. **Managing collateral within a Probe Image:** The RFR System has the ability to select relevant faces for RFR Searching where an image has multiple people within it prior to any biometric processing having occurred.
- c. **Source / Expectations of Privacy:** the need to consider the source of Probe Images including (i) the source of the image and any risk of compromise/risk to that source, (ii) where the image is taken of a non-compliant subject, raises wider human rights consideration or otherwise obtained in circumstances where there are greater expectations of privacy. The use of the Probe Image ‘Levels’ system and the elevated privacy considerations position in the MPS RFR Policy Document embeds this approach.
- d. **Currency:** controls around the currency of Probe Image with the most up to date and/or suitable image being used for RFR Searching unless there are particular reasons to search against a specific image.
- e. **Suitability:** ‘by design’ the RFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate responses.
- f. **Use:** Probe Images may only be used for RFR Searching if they fall within specified categories which each link to an underlying policing purpose and ground. Further specific safeguards have been adopted in relation to age, relevant disability and those who have and/or are undertaking a gender reassignment.

---

<sup>17</sup> (2009) 48 EHRR 50



- g. **Ongoing searching:** The criteria for addition to the Unresolved Crime Cache and the time-limited periods before a review is required ensures a continued need to see a Potential RFR Match is made out.
- h. **Additional retention controls:** The MPS has adopted MOPI controls as regards retention, but supplemented this with further control measures based around how the system operates to ensure retention is focused and proportionate in the context of the MPS's use case for RFR. This process ensures that where data is not needed within the RFR System is removed from it.

2. Image Reference Images:

- a. **Methodology for use:** the selection of the Image Reference Libraries for searching is specific to each RFR Search and informed by the intelligence case and policing need for that RFR Search; this is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching.
- b. **Ad-Hoc image Reference Libraries:** the use of a limited-time, limited-purpose and access controlled Image Reference Library to limit the availability of images relevant to a specific investigation or operation from wider searching.
- c. **Additional retention controls:** The MPS has adopted MOPI controls as regards retention, but supplemented this with further control measures to ensure the images retain currency and are proportionate in the context of the MPS's use case for RFR. This has also informed the MPS's dedicated retention periods for those who are aged under 18. These controls are specific to the use of data processed by the RFR System and are distinct from any controls that apply to the retention of the underlying images held by the police.
- d. **Designed in deletion:** In relation to Image Reference Libraries, these are not dedicated resources just within the RFR System and will be retained by the MPS in line with the policy applicable to them (save that in some cases additional safeguards may be put in place to ensure proportionality). From an RFR perspective, images imported via the 'delta link' to an Image Reference Library will cease to be available for RFR Searching 'by design' if the underlying image is deleted. Additionally images will be deleted from any RFR system on expiry of any approval to use the Image Reference Library for RFR Searching.
- e. **Human in the loop:** the RFR system is designed to assist MPS personnel. The RFR system will always flag potential matches against an Image Reference Library 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.

3. Approvals for RFR Searching: the MPS has adopted a system where a level of approval is needed in order to return an RFR Search result – the level being proportionate to the expectations of privacy that are associated with the relevant imagery:

- a. **Image Reference Libraries:** prior to the utilisation of any Image Reference Library for searching by means of Probe Image the an approval must be obtained from: (i) the MPS RFR SRO in the case of Substantive Image Reference Libraries; or (ii) an officer of at least Superintending rank in the case of an Ad-Hoc Image Reference Library (save in cases of urgency). This provides oversight and scrutiny from suitably senior personnel with experience of evaluating the policing need with the intrusions associated with a policing action.
- b. **Probe Images:** RFR Users are able to undertake RFR Searches using Probe Images with the lowest levels of intrusion against Image Reference Libraries that have been approved for RFR Searching. To run an RFR Search using a more sensitive Probe Images the approval of at least Inspecting rank is required – such officers are familiar with privacy considerations and in other contexts, such as custody are already given legal powers under PACE for authorising the taking of other biometric data and undertaking searches using it.

#### 4. Review:

- a. **RFR Search results:** All RFR Searches are subject to human-in-the-loop decision making – a Potential RFR Match only becomes a Viable RFR Match following a human review via the Adjuration process.
- b. **Approval and review of Image Reference Libraries:** The MPS RFR Policy provides as means by which the SRO and the FR Board will be cited as regards the Image Reference Libraries used within the MPS RFR System.
- c. **Ongoing:** RFR Searching and the materials that support RFR Searches will be subject to periodic review to ensure that the RFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case.

**Key point:** When taking a decision to use RFR, the proportionality decision needs to balance the policing need with the impact on individual rights. This should include having regard to particular privacy considerations that may be relevant to a Probe Image or the use of a particular Image Reference Library. This may include factors such as where the image was taken, how it came into police position its revelatory effect location and the actions taken to date prior to undertaking an RFR Search.

### 3.20 Wider Human Rights Act considerations

- (a) The right to privacy is a value that 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 also be particularly relevant in the context of RFR.
- (b) **Article 9** - the clothing people wear, the places people attend, the actions people take may all, on occasion, be discerned from imagery and can be an act of thought, conscience and

religion. Additionally, some imagery may reveal a range of non-religious beliefs including atheism, agnosticism, veganism and pacifism. Article 9 provides:

*Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching practice and observance.*

*Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society:*

- *in the interests of public safety,*
- *for the protection of public order,*
- *health or morals, or*
- *for the protection of the rights and freedoms of others.*

**Example:** Should a violent street crime occur outside a place of worship targeting worshipers leaving the premises, the images and CCTV video excerpts from the place of worship may be important to successfully investigating that crime and prosecuting the perpetrators. RFR would be a valuable tool in this context to identify the perpetrators but also to determine their previous behaviour and whether they had made previous visits to the site to plan their crime. It would compare favourably to manually reviewing footage in terms of bring people who pose a risk to public safety to justice swiftly. It would also provide a greater assurance as to the planning process and the people involved in such an attack. In this context, whilst RFR would avoid the need for the police to manually review the footage and therefore study all worshipers to assess their relevance to the investigation, RFR will undertake some processing against all those in the footage (be simply face detection or where thought necessary, further biometric processing against an Image Reference Library). Any impact would need to be weighed against the public safety policing objectives to be sure the course of action is necessary and proportionate. In this respect, it is notable that the successful investigation using RFR in a limited way, for a limited time would actually help protect worshipers in the future and therefore enable them to exercise their Article 9 rights.

**Article 10 and 11** have particular relevance when considering the policing of assemblies and demonstrations and RFR has potential to impact on an assembly or demonstration or the willingness of people to exercise their Article 10 and 11 rights in the future.

Article 10 enshrines a right to freedom of expression. This right includes the freedom to hold opinions, and to receive and impart information and ideas, but allows restrictions which in accordance with law and necessary in a democratic society for:

- interests of national security;
- territorial integrity or public safety;
- prevention of disorder or crime;
- protection of health or morals;
- protection of the reputation or the rights of others;
- preventing the disclosure of information received in confidence; and
- maintaining the authority and impartiality of the judiciary.

Article 11 protects the right to freedom of assembly and association, including the right to form trade unions, subject to certain restrictions that are in accordance with law and necessary in a democratic society. Interference with Article 11 may be justified for:

- interests of national security;
- public safety;
- prevention of disorder or crime;
- protection of health or morals; and
- protection of the reputation or the rights of others.

(c) *Operational Duties*

The ‘operational duty’ was first outlined in the case of *Osman v United Kingdom*<sup>18</sup> and concerned an alleged failure to prevent the young victim and his family from the risk to life posed by a stalker. The European Court of Human Rights in *Osman* found that the police were under a positive duty to take reasonable measures to avert a real and immediate risk to the life of an identified individual or individuals of which the police were, or ought to have been aware. Caselaw also supports that the police are under an *Osman* style duty to investigate serious allegations in a timely and efficient manner in order to uphold an individual’s Article 3 rights.

The *Osman* operational duty has particular relevance to RFR in two contexts (i) being used to aid investigations of those posing a threat to the public or themselves where a real and immediate risk to life is identified and RFR is thought to provide a key tool to aid or accelerate an policing investigation and (ii) on a Potential RFR Match being generated where the need to Adjudicate and respond to the results may engage the *Osman* operational duty.

## 4 Equality Act 2010

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

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

The Court of Appeal *Bridges* decision makes it clear that the PSED requires the MPS to take reasonable steps to satisfy itself, either directly or by way of independent verification, that the algorithm in this case does not have an unacceptable bias on grounds of race or sex. The need to be informed as to the performance of the algorithm also applies to the use of a RFR

---

<sup>18</sup> [1999] 1 F.L.R. 193 (ECtHR)

system. To assist the public with understanding how the MPS meets its PSED duties, the MPS has published the MPS RFR Equality Impact Assessment. Additionally, the MPS has published a paper entitled 'Understanding the Metropolitan Police Service RFR System's Accuracy and Bias Position'. This explains the steps the MPS has taken to understand the statistical accuracy and demographic performance of its RFR algorithm. This includes:

1. **Independent evaluation:** A number of studies highlight the varying performance of facial recognition algorithms and the potential for the performance of algorithms vary dependant on demographic factors. As a result the MPS has paid regard to the evaluations undertaken by the National Institute of Standards and Technology (NIST) who have evaluated circa 200 facial recognition algorithms for statistical accuracy and demographic performance, including those submitted by NEC – the provider used by the MPS.
2. **Peer review:** The MPS's position paper has been reviewed by other experts in the field including the Defence Science and Technology Laboratory and the National Physical Laboratory.
3. **Ongoing assurance:** The MPS RFR Documents provide for ongoing evaluation and a review process. This reflects the ongoing nature of the PSED duty and also offers the MPS a chance to monitor for technical issues by reviewing performance and monitoring for trends. Should a concern be identified, the MPS would then be in a position to explore that further and test for issues under the oversight and scrutiny of the MPS Facial Recognition Strategic Board.

(b) *The use of the RFR system.*

As a result of having taken reasonable steps to understand the statistical accuracy and demographic performance of the MPS RFR System and then in light of points relating to subject, system and environmental factors, the MPS has adopted a 'fail-safe' position to ensure that absent there being other lawful grounds to take policing action:

**Potential RFR Matches returned will be subject to human in the loop Adjudication prior to the result being assessed to be a Viable RFR Match.**

This means the RFR system is not making any decision. The nature of a Viable Match is not a definitive confirmation of identity or that the subject in the two images is actually the same person. It follows that a Viable Match should be treated as an intelligence lead for further investigation.

Similarly those undertaking the Adjudication are best placed to consider the impact of any factors which may have influenced the RFR system when it generated a Potential RFR Match and if such factors combine to mean that further action is not appropriate in the circumstances.

MPS personnel are also familiar with managing the PSED requirement whilst undertaking policing activities from a number of other crime fighting techniques. The Equality Impact

Assessment informs the use of RFR to mean the MPS upholds the Public Sector Equality Duty. Compliance with the Equality Impact Assessment should then be monitored and reviewed to reflect the ongoing nature of the PSED.

## 5 Data Protection Act 2018

- 5.1 The MPS processes personal data for RFR ‘based on law’ - specifically its legal powers identified in relation to the common law as well as human rights and equality considerations as outlined in this Legal Mandate, and the policies put in place by the MPS RFR Documents. The Appropriate Policy Document and other MPS RFR Documents published by the MPS as a public body allows the public who may be subject to RFR processing to understand the standards the MPS operates to, including setting out the authorisation process and requirements to use RFR, and the considerations and constraints relevant as to when Probe Images and Image Reference Libraries may be used for RFR Searching.
- 5.2 For the purposes of preventing crime and disorder, Part 3, Data Protection Act 2018 (DPA) regulates the processing of personal data, including sensitive processing, whether processed on a computer, CCTV, still images or other media. Any recorded image from a device which can identify a particular person is ‘personal data’. The DPA therefore applies to the processing of data for RFR in relation to both Probe Images and Image Reference Libraries. These actions are covered by the processing of data for law enforcement purposes, as defined in s.31 DPA:

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

**Key point:** Those using and approving the use of RFR need be satisfied of the necessity to use RFR 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 RFR system’s processing of biometric data is strictly necessary for the law enforcement purpose. The law enforcement purpose should be clearly identified and the way in which the strictly necessary standard has been met explained.

- (a) Strictly necessary in this context means that the processing has to relate to a pressing social need, and it is not reasonably viable to address this through less intrusive means. Any personal data collected via RFR is not used in a manner that is contrary to the identified law enforcement purpose.
- (b) The ‘strictly necessary’ standard may be informed by considering factors including:
- (i) what other policing methods (including those that do not require sensitive processing to be undertaken) have been used / discounted;
  - (ii) the importance of achieving the law enforcement purpose and the prospects of achieving the law enforcement purpose through the use of RFR using the Probe Image and the Image Reference Libraries;
  - (iii) the size and scale of the planned RFR Search the level of sensitive processing anticipated – for example is it a single Probe Image or multiple images, is it for a single processing need or an ongoing need based on the Unresolved Crime Cache; *and*

- (iv) if the law enforcement purpose which underpins the use of RFR is strictly necessary and proportionate to the need to undertake sensitive processing and the risk to individuals' rights this entails (subject to the protections and safeguards implemented).

**Key point:** Those using and approving the use of RFR need to be satisfied that the processing satisfies one of the Schedule 8 conditions set out below and complies with the six data protection principles.

### 5.3 Schedule 8 conditions of the DPA are:

- necessary for judicial and statutory purposes – for reasons of substantial public interest;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; *and*
- necessary for archiving, research or statistical purposes.

**Example:** The use of RFR will assist the MPS in fighting knife and gun crime in support of its common law policing powers. RFR could be used to establish that the photo of a subject with a knife in a current investigation is also wanted for previous offences. Used in this way, RFR would assist in the prevention, investigation, detection or prosecution of criminal offences.

RFR offers advantages over other potential policing methods, for example undertaking local enquiries with policing colleagues as to their knowledge of the subject. This risks only a partial information, especially when criminality occurs across geographical areas in London.

Given the importance of tackling serious and violent crime, a clear law enforcement purpose can be identified. In this context RFR's use may be seen as strictly necessary to support the investigation of knife and gun crime, to enable the MPS to effectively respond to a pressing social need.

Similarly, the Schedule 8 condition of being necessary for judicial and statutory purposes for reasons of substantial public interest can be seen in this context to include a police officer working for the prevention, investigation, detection or prosecution of offences to keep the public safe.

5.4 The MPS has also undertaken a number of steps in accordance with the Data Protection Impact Assessment (DPIA) to manage and mitigate the impact of any personal data processing using the RFR system. Particular actions are set out in the remainder of this section.

### 5.5 Data Protection Impact Assessment:

A DPIA has been conducted to support the use of RFR in order to identify and minimise the data protection risks. Whilst the overall DPIA will be reviewed annually, those approving the use of an Image Reference Library for the use of RFR should ensure there all aspects of a particular Image Reference Library and the Probe Images which may be used to search it are covered and the risks to data subjects mitigated as far as possible by the DPIA.

#### 5.6 Data Protection by Design:

A number of data protection controls have been designed into the RFR system in order to mitigate processing impacts on privacy and to comply with the general obligation in Part 3 of the DPA to implement appropriate technical and organisational measures having considered and integrated the principle of data protection into RFR processing activities. The designed-in measures identified at paragraph 3.19(c) of this document, include measures to:

- (a) limit the amount of personal data collected;
- (b) limit the extent of personal data processing;
- (c) limit the period of personal data storage.

Additionally, the MPS has acted to ensure that the RFR system performs to a level where the statistical accuracy of the data being processed and fairness 'by design' is ingrained into the MPS's RFR system. The MPS RFR Documents and other published supporting information explain how the MPS is assured that its RFR system operates with a high degree of statistical accuracy and in a way that does not lead to unjust results between demographics.

The RFR system also includes a number of physical and technical security measures including:

- All data processed by NeoFace Reveal internally is secured through data encryption.
- All data at rest is encrypted including biometric templates
- Standard Foundation accounts will be used to manage each MPS user's identity for NeoFace Reveal. MPS Single Sign-On will be enabled.
- Access is restricted to authenticated and authorised MPS users, based on an RBAC model.
- Timeouts will be configured as required. It is recommended that user sessions timeout after a set period of inactivity and after a set number of hours regardless of activity.
- The NeoFace Reveal application has native antivirus scanning functionality and all files uploaded will be scanned
- A security incident and response process including cyber breaches applies.

#### 5.7 Appropriate Policy Document:

Section 42 of the DPA requires that, at the time that the processing is carried out, the controller has an appropriate policy document in place. The MPS has produced this document and published it. This document allows the public to understand details of the:

- (a) the data being processed by the RFR system, how often it is processed and whose data is processed;
- (b) procedures, safeguards and accountability principles for complying with the data protection principles when relying on a condition from Schedule 8 to process biometric personal data both in relation to Probe Images and Image Reference Libraries;
- (c) MPS policy for the retention and erasure of personal data for RFR processing.



## 5.8 Data Protection Officer:

The MPS has appointed a Data Protection Officer (DPO) in compliance with Part 3 DPA who has been consulted in relation to RFR. The DPO is available to inform and advise the Commissioner (as data controller) and MPS personnel about their obligations in relation to the DPA. The DPO also provides an internal function to monitor compliance with the DPA.

## 6 Legal considerations regarding using RFR in relation to the deceased

6.1 The use of RFR Searching to facilitate the identification of the deceased raises particular legal considerations.

(a) Data protection considerations: The DPA applies to information that relates to identifiable living individuals. Information relating to a deceased person does not constitute personal data and is therefore not subject to the DPA albeit the need to act with empathy and respect remains paramount. There may still be circumstances where an RFR Search results cause the police to link the deceased to sensitive information. In this respect, care still needs to be taken from a legal perspective notwithstanding that the data is not 'personal data' for data protection purposes after death. This is because information provided subject to confidentiality obligations can see those confidentiality obligations endure beyond a person's death.

(b) Human rights considerations: The exercise of Article 8 rights concerning family and private life pertains, predominantly, to relationships between living human beings. Article 8 can however still have relevance and application to the police seeking to identify the deceased:

(i) **Informing the family:** The case of *Lozovyye v Russia*<sup>19</sup>, for instance concerned a murder victim who had been buried before his parents had been informed of his death. In that case, the Court reiterated that everyone had a right to access to information relating to their private and/or family life and that a person's right to attend the funeral of a member of their family fell under Article 8. The courts have recognised there is an obligation for the authorised to at least undertake reasonable steps to ensure that members of the family are informed of a death and any funeral arrangements. In this light, RFR can assist the police in facilitating the prompt identification of the deceased which in turn can support informing family members.

(ii) **Treatment of the deceased:** Whilst Article 8 is focused on the private and family life of living human beings, as recognised in *Putistin v Ukraine*<sup>20</sup> the "right to respect for the honour and dignity of a deceased relative is an element of the right to respect of private life guaranteed by Article 8". The case was considered in the context of defamation, even after the defamed party has died. It recognises that the courts might sometimes be required to protect the reputation of the deceased in the interests of surviving relatives. From a policing perspective, it is important to be mindful of the potential for

---

<sup>19</sup> (*Application no. 4587/09*), 24 April 2018.

<sup>20</sup> (*Application no. 16882/03*), 21 November 2013.

impact on the deceased's living relatives when seeking to identify a subject – acting with empathy and respect. In this respect RFR offers a non-invasive mythology to assist with this process.

## **7 Freedom of Information Act 2000**

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

- (a) public authorities are obliged to publish certain information about their activities;
- (b) members of the public are entitled to request information from public authorities.

In recognition of its FOIA duties, the MPS makes significant RFR information available via its website. The MPS will also be responsive to FOIA requests.