Suitable for Publication	Yes
Title and Version	Live Facial Recognition, (LFR) MPS Legal Mandate.
Purpose	To outline the legal position of the MPS with regards to the use and deployment of Live Facial Recognition technology as an overt policing tactic.
Relevant to	MPS SC&O35, NPCC, DLS, DMC, SCC, ICO, BC, MOPAC and other key Stakeholders.
Summary	This document outlines the legal and regulatory frameworks, together with the ethical considerations in which it is operating in the use and deployment of LFR..
Author and warrant/pay number	DSU Bernie Galopin 195523, DI Nigel Nelson 188691.
Creating branch	SC&O35
Date created	23.07.2018
Review Date	23.07.2019
Circulation List	To be determined by MPS NPCC

Contents

Introduction

The MPS is currently undertaking trials within different environments and policing operations in order to assess the situations under which LFR technology can be used as a viable and effective policing tactic.

At the conclusion of all the trial deployments, the results will be assessed and analysed by both by the MPS and accredited by an independent authority. The evaluation will focus on the effectiveness, efficiency and practicality of LFR technology and an operational evaluation of such technology for policing purposes. A public consultation will then be held in order to discuss the police use of LFR and to canvass public concerns about the use of this technology.

This Legal Mandate outlines the position of the MPS with regards to the use and deployment of Live Facial Recognition as an overt policing tactic. This document outlines the legal, regulatory frameworks and ethical considerations that the MPS is adhering to with regards to LFR.

LFR trials

Strategic Intentions

1. To implement a command structure which incorporates strategic, operational and technical leads for the development, promotion, advancement and evaluation of the use and deployment of LFR technology within the MPS. The board will be the single point of governance for all proposed live facial recognition capability.
2. To identify and evaluate an evidence base from which the overt use and deployment of LFR technology will lead to a comprehensive assessment of LFR as a policing tactic.
3. To ensure that the overt use and deployment of LFR for policing purposes meets the oversight and regulation framework outlined in the UK by the Surveillance Camera Commissioner, the Biometrics commissioner and the Information Commissioners and to ensure that all relevant legislative provisions are complied with.
4. To ensure that reputational and organisational risk for the MPS are identified, managed and mitigated effectively.
5. To build trust and confidence amongst London's communities through the overt use and deployment of LFR technology for policing purposes.
6. To build trust and manage relations effectively with all key stakeholders concerned in the protection of privacy and human rights that may be impacted by the use of LFR technology through the use of an effective Stakeholder Engagement Strategy.
7. To ensure that communication with all relevant stakeholders and the general public is managed effectively through a comprehensive Press and Media Strategy.

Operational Objectives

1. To maximise opportunities within the UK to trial (10 events) the overt use and deployment of LFR technology for policing purposes.
2. To establish and resource an MPS LFR Team which will liaise effectively with command teams in the planning, briefing and deployment of LFR technology at selected events.
3. To work effectively with operational teams within the MPS, other police forces and with selected partners to ensure that events are appropriately supported with shared resources and capabilities.
4. To use LFR technology to reduce and disrupt crime and to increase enforcement opportunities at selected events.
5. To provide reassurance to communities at the selected events that the MPS are utilising innovative and effective approaches to policing.
6. To increase satisfaction and confidence within London's communities by listening and responding to local concerns in regards to the overt use and deployment of LFR technology at events.
7. To adopt a robust, proportionate and intelligence initiated approach in engaging and pursuing individuals identified on the 'watch list' at selected events.

Technological Objectives

1. To ensure that all LFR technology is fit for purpose and deployed effectively in line with the strategic intentions and operational objectives.
2. To provide technical oversight for all proposed use cases, trials & evaluations of live facial recognition capability.
3. To conduct an evaluation into the effectiveness and suitability of the overt use and deployment of LFR technology as a policing tactic.

Legal Framework

The legal framework for the use and deployment of LFR is summarised below:

- Common Law
- Human Right Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Data Protection Act 2018

Common Law

The police can, in fulfilling its operational duties, conduct themselves in a manner which is not contrary to law. These core principles are outlined below:

- Protecting life and property.
- Preserving order.
- Preventing the commission of offences.
- Bringing offenders to justice.

Human Rights Act, (HRA) 1998

Utilisation of LFR technology has the potential of impacting upon Article 8: Right to respect for private and family life.

"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".

The MPS ensures compliance with HRA legislation in respect of the deployment of LFR technology as the principles of Proportionality, Legality, Accountability and Necessity are all adequately satisfied:

Proportionality:

1) The authorisation will not be proportionate if it is excessive in the overall circumstances of the case.

   The aims and objectives of this operation are to identify individuals who are wanted by the police and the criminal justice systems and to utilise LFR with a view to apprehending them and reduce the prevalence of crime within the relevant area. It is right and appropriate to bring people who are unlawfully at large to justice as they may otherwise pose a threat of safety to the public through the commission of crime.

2) Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

   This approach is less intrusive than other methods of tracing wanted persons. It is less resource intensive which will save police time and money and allow police to concentrate resources on other priorities.

3) The fact that the suspected offence may be serious will not alone render intrusive actions proportionate.

   This is less intrusive than other methods and this approach is wholly appropriate to apprehend individuals who are wanted. The methodology used and safeguards which are in place make this a viable and proportionate option.

4) An offence may be so minor that any deployment of covert techniques would be disproportionate.

   This methodology applies to overt policing principles.

5) No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

Previously, other methods have been employed and proved to be inadequate. These methods have included visiting addresses of the wanted person or their families and associates, developing police intelligence databases or using intelligence generated from parties to facilitate locating them. LFR is likely to be more effective and efficient as it does not rely on information sharing with other agencies.

Accountability:

The MPS will hold an Advisory, Consultation and Oversight Group, (ACOG) to ensure that there is a full consultation process and to ensure that any decisions which are undertaken will be made in an open and transparent manner. The ACOG has links with other oversight groups and key stakeholders.

An organisational learning mandate has been developed, responsible for the collation of developmental concerns which have been highlighted by internal and external stakeholders. Risks are captured and escalated through formal processes.

Systems and processes are in place to ensure the effective management of the trials with full audit trails to evidence transparency.

Governance relating to the LFR trials is outlined in this Legal Mandate which will be shared with regulators, key stakeholders and the public.

Necessity:

LFR technology meets the MPS's core principles in policing:

- Protecting life and property.
- Preserving order.
- Preventing the commission of offences.
- Bringing offenders to justice.

It is necessary to conduct the trials in line with the strategic intentions, operational and technical objectives and to conduct a comprehensive evaluation (internal and external). This will contribute to the understanding of the overt use of LFR and how it presents a viable policing tactic.

LFR is deployed in areas where there are particular crime issues, such as those with serious violence, knife crime and gang activity or at public events where risks need to be managed effectively.

A principal purpose of this technology is to apprehend wanted offenders and in doing so to prevent, deter and reduce the incidence of crime through bringing those who are unlawfully at large to justice. Each deployment will be underpinned by a comprehensive intelligence case to highlight the need to combat the relevant crime issues.

Safeguards Against Collateral Intrusion:

LFR technologies are aimed at identifying data held on a bespoke watch list with data captured through live recording apparatus. All data which is not matched is discarded immediately. Data which is matched with that on the watch list is retained for 30 days.

The safeguards around human intervention will reduce collateral intrusion as decision making is wholly reliant on the police officer. This methodology is a less intrusive

approach than other methods used by police to trace persons who are unlawfully at large.

Data Protection Act 2018

Part 3 of the DPA 2018 makes provision in relation to the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.

Sections 35 – 40, (Principles 1 – 6) Data Protection act 2018 are adequately responded to within Section 6, (Pages 1 – 6) of the Data Privacy Impact Assessment. Sections 35 - 40 are listed as:

Section 35: the processing of personal data for any of the law enforcement purposes must be lawful and fair.

Section 36:
a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and
b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

Section 37: personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Section 38:
a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and
b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

Section 39: that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

Section 40: that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

The DPA 1998 was used as a point of reference for the Privacy Impact Assessments conducted for the first three trials. The DPA 2018, which was enacted by Parliament on 25th May 2018, and has been used as underpinning legislation for the Data Protection Impact Assessment which was last verified by Commander Ivan Balhatchet, MPS Strategic lead for LFR and the MPS Data Protection Officer on 14th June 2018. In compliance with the ICO code of practice it is reviewed before every deployment and accordingly considered to be a "living document".

Risks are considered under Section 64 Data Protection act 2018 and are adequately responded to within Section 7, (Pages 13 – 15) of the Data Protection Impact Assessment, (DPIA).

The MPS has designated a Senior Responsible Officer, (SRO) with strategic responsibility for ensuring compliance with the SC Code of Practice.

Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 has the following areas of relevance to LFR:

- Part 1 - Section 20 of Chapter 1 instructs the Secretary of State to appoint a Commissioner, to be known as the Commissioner for the Retention and Use of Biometric Material, to review the use and retention of biometrics by the government.

- Part 2 - Chapter 1 creates new regulation for, and instructs the Secretary of State to prepare a code of practice towards closed-circuit television.

The effect of the code for security camera surveillance systems is of significant relevance to the LFR trials and is highlighted under Section 33 PoFA 2012, sub-sections 1 – 4;

(1) A relevant authority must have regard to the Surveillance Camera Code when exercising any functions to which the code relates.

(2) A failure on the part of any person to act in accordance with any provision of the Surveillance Camera Code does not itself make that person liable to criminal or civil proceedings.

(3) The Surveillance Camera Code is admissible in evidence in any such proceedings.

(4) A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the Surveillance Camera Code in determining a question in any such proceedings.

The requirements of the Protection of Freedom Act 2012 are covered by the Surveillance Camera Code of Practice 2013.

Freedom of Information Act 2000

The Freedom of Information Act 2000 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; and
- members of the public are entitled to request information from public authorities.

The MPS has received a number of Freedom of Information Act requests to date specific to LFR deployments and its technology. All FoIA requests are currently dealt with by the

MPS FoIA Manager, who maintains a publication scheme in respect of the nature and subsequent management of requests. All requests are forwarded to DSU Galopin, MPS Operational lead for LFR, who pass on all completed requests to the reviewing officer, Commander Balhatchet prior to a response being made to the applicant.

The MPS LFR team has a database upon which all FoIA requests are logged and their process managed. This in particular assists responding to common questions asked in that a standard response can be provided on the basis of responses to previous requests.

Regulatory Framework

In terms of oversight and regulation of LFR use, there are three strands relevant to England & Wales:

Surveillance Camera Commissioner (SCC):

The SCC has no statutory powers in England and Wales but operates with a voluntary Code of Practice. The MPS complies with this code through its Self- Assessment. The SCC Self- Assessment tool kit was last updated by the MPS in November 2017.

The Security Camera Commissioner does however provide appropriate and effective guidance in respect of the use of overt surveillance systems. The MPS should follow a duty to have regard to the guidance within the Surveillance Camera Code of Practice when deploying surveillance cameras in public places.

Section 2.6.1-12, identifies 12 guiding principles which system operators should adopt. These are responded to within the SCC Self-Assessment tool. This needs to be reviewed prior to each LFR deployment to ensure that the principles and underlying legislation are complied with.

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is

granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Where joint operations are being undertaken, Section 3.4.2 needs to be complied with:

"Where a system is jointly owned or jointly operated, the governance and accountability arrangements should be agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance".

Biometrics Commissioner (BC)

The Biometric Commissioner's Office was created by the Protection of Freedoms Act, 2012 (PoFA) to provide assurance to the Home Secretary and to Parliament on the working of that legislation. The PoFA granted the Biometrics Commissioner oversight and some limited decision making powers as regards to the retention and use of biometrics, which includes data retained as a consequence of LFR technology. The BC has been consulted throughout the LFR pilots and has provided guidance in respect of the retention, removal and disposal of biometric data. The Biometrics Commissioner has produced a series of general ethical principles which are applicable to the LFR trials. These have been incorporated within the Operational Learning Mandate.

1. Trials are only justified to provide new knowledge necessary to consider possible future deployment of a capability.

2. These principles apply to the design and execution of trials of the use of facial search and matching technologies in public spaces in order evaluate the utility and limitations of any use for later operational purposes. They do not apply to operational use of the same technology where quite different issues apply.

3. It is crucial that public trust in the police use of biometric based identification systems exists if they are to be seen as legitimate and therefore a general principle of transparency should apply when conducting trials.

4. The public should be informed and consulted when a trial, or series of trials is to be conducted and the purpose and general approach to evaluation explained.

5. The public should be informed at a trial location that a trial is in progress and given a contact where further information can be found/requested.

6. The public should be informed as to the general results of trials.

7. All trials should be properly evaluated in order to produce new knowledge about any possible operational future use. Good practice would be to have results peer reviewed by external scientists.

8. Evaluation should include not just the identification and matching capabilities of the system being trialled but also what processes would be required to ensure that any matching claims can be properly authenticated and evidenced if such a system were used operationally.

9. Any data collected as part of the trial which allows individual identification should only be kept until the evaluation is completed or for a short period after the conclusion of the trial. At the end of that period it should be destroyed.

10. All data collected during a trial should be securely stored in such a way as to allow access only to those conducting the evaluation.

11. Trials will be discrete and limited in scope. Any extension to wider operational use is not permitted without it fulfilling legal requirements and separate additional principles of governance being applied.

12. The police force conducting a trial will share their detailed results with the rest of the police service via the NPCC lead for biometrics, presently CC Debbie Simpson.

Information Commissioner's Office (ICO)

The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Data Information Privacy Assessment which complies with Sections 35 – 40, (Principles 1 – 6) and Section 64 Data Protection Act 2018 has been shared with the ICO on 28th July 2018. This document has been published by the MPS.

Ethical Considerations

Ethical Considerations outlined by RIPA

Safeguards are considered under the principles of justification, proportionality, necessity and collateral intrusion as applied to RIPA 2000. Although LFR is deployed in overt conditions, principles associated with RIPA are set as standards in order to demonstrate that surveillance principles have been considered with a view to ensuring that ethical principles have been satisfied.

Regulatory Investigative Powers Act 2000, (RIPA provides direction with regards to covert surveillance) but has been considered within this framework in the context of guiding principles for consideration regarding the use of overt surveillance tactics.

Specifically, Sections 3.5 and 3.6 of the Surveillance and Property Interference Codes of Practice (Published 2014) relate to Proportionality in respect of granting surveillance authorisations:

Section 3.5, Generals Rules of authorisations relating to Necessity and Proportionality:

- The authorisation will not be proportionate if it is excessive in the overall

circumstances of the case.

- Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary
- The fact that the suspected offence may be serious will not alone render intrusive actions proportionate.
- An offence may be so minor that any deployment of covert techniques would be disproportionate.
- No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

Section 3.6, Generals Rules of authorisations relating to Necessity and Proportionality:

- Balancing the size & scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

Safeguards to ensure ethics are protected

Ethical considerations are furthermore satisfied through the human intervention principles which are used at LFR deployments with a view to ensuring that quality assurance checks are undertaken in respect of the generation of positive alerts.

The MPS has formulated an Advisory Consultative Group, (ACG) in July 2018, whose terms of reference are noted:

- provision of advice to the MPS.
- a platform to promote engagement and consultation between the MPS and key stakeholders with a strong interest in LFR and who can influence and shape the future use and deployment of it. To promote opportunities to engage with other stakeholders, particularly the public.
- a basis for exchanging and sharing information within defined parameters (MOU).
- opportunities for police forces to collaborate effectively in the use and deployment of LFR and to identify and implement best practice into operational environments.
- a mechanism of reporting into the Home Office oversight board and to the NPCC lead.
- to promote ethical considerations within a legal, regulatory frameworks.

The ACOG aspires to develop and promote open and honest transparent discussion between the MPS and its constituent members, including regulators and key Stakeholders including MOPAC with respect to the LFR pilot process.

Ethical considerations are furthermore responded to through the development of a MPS LFR web site, intranet site, press and media strategies giving advance disclosure of

deployments and branding and the distribution of leaflets at events providing information and seeking feedback via e-mail.

Operational briefings delivered to officers and stakeholders prior to deployments likewise have the common strand of openness and honesty and officers are directed to offer leaflets to the public and fully engage with them in order to increase awareness of LFR as a policing tactic.

A Continuous improvement and organisational learning process has been created to collate feedback from both internal partners, external stakeholders and the public with a view to ensuring that any areas of development are identified at the outset and mitigating factors introduced in order to enhance efficiencies. Best practice is also identified and promoted throughout these processes.

Key Stakeholders are invited to observe to observe the planning and deployment of the LFR trials.